ZyWALL USG
ZLD 2.21 Support Notes

Revision 1.00

August, 2010

Written by CSO

Table of Contents

Scenario 1 — Connecting your USG to the Internet 4
1.1 Application Scenario 4
1.2 Configuration Guide 5
Scenario 2 — WAN Load Balancing and Customized Usage of WAN Connection for Specific Traffic 12
2.1 WAN Load Balancing 12
2.1.1 Load Balancing Algorithm 12
2.2 Customized Usage of WAN Connection for Specific Traffic Type 14
2.3 Application Scenario 15
2.4 Configuration Guide 16
Scenario 3 — How to configure NAT if you have Internet-facing public servers 22
3.1 Application Scenario 22
3.2 Configuration Guide 23
Scenario 4 — Secure site-to-site connections using IPSec VPN 27
4.1 Application Scenario 27
4.2 Configuration Guide 28
Scenario 5 — Secure client-to-site connections using IPSec VPN 35
5.1 Application Scenario 35
5.2 Configuration Guide 36
Scenario 6 — Deploying SSL VPN for Tele-workers to Access Company Resources 45
6.1 Application Scenario 45
6.2 Configuration Guide 46
Scenario 7 — Reserving Highest Bandwidth Management Priority for VoIP Traffic 55
7.1 Application Scenario 55
7.2 Configuration Guide 56
Step4. Create a bandwidth management rule and configure 60

All contents copyright (c) 2010 ZyXEL Communications Corporation.

Scenario 8 — Reserving Highest Bandwidth Management Priority for a Superior User and Control Session per Host 61
8.1 Application Scenario 61
8.2 Configuration Guide 62
Scenario 9 — Using ZyWALL to Control Popular P2P Applications 71
9.1 Application Scenario 71
9.2 Configuration Guide 72
Scenario 10 — Deploying Content Filtering to Manage Employee Browsing Behavior 77
10.1 Introduction to ZSB (ZyXEL Safe Browsing) 78
10.2 Application Scenario 78
10.3 Configuration Guide 79
Scenario 11 — Quick Setup for Allowing WLAN Users to Access LAN Services 86
11.1 Application Scenario 86
11.2 Configuration Guide 87

All contents copyright (c) 2010 ZyXEL Communications Corporation.

Scenario 1 — Connecting your USG to the Internet

1.1 Application Scenario

A WAN (Wide Area Network) connection is an outside connection to another network or the Internet. It connects your private network such as LAN (Local Area Network) and other networks, so that a computer in one location can communicate with computers in other locations.

The USG has a multiple WAN feature which enables you to link your network with up to two ISPs or other networks via Ethernet, PPPoE or 3G connections. User can either use trunks for WAN traffic load balancing to increase overall network throughput ("active-active" load sharing mode) or as a backup to enhance network reliability ("active-passive" failover mode).

Load balancing will be described further in Scenario 2. In the figure below we first show the scenario for non-stop Internet access with the PPPoE as primary WAN and 3G backup through USB. This means that the USG will normally use the PPPoE interface for Internet access, and it will only resort to the 3G interface when the PPPoE interface's connection fails.

All contents copyright (c) 2010 ZyXEL Communications Corporation.

1.2 Configuration Guide

Network Conditions:

USG-50:

- WAN1_PPP: PPP over Ethernet
- Cellular1: 3G

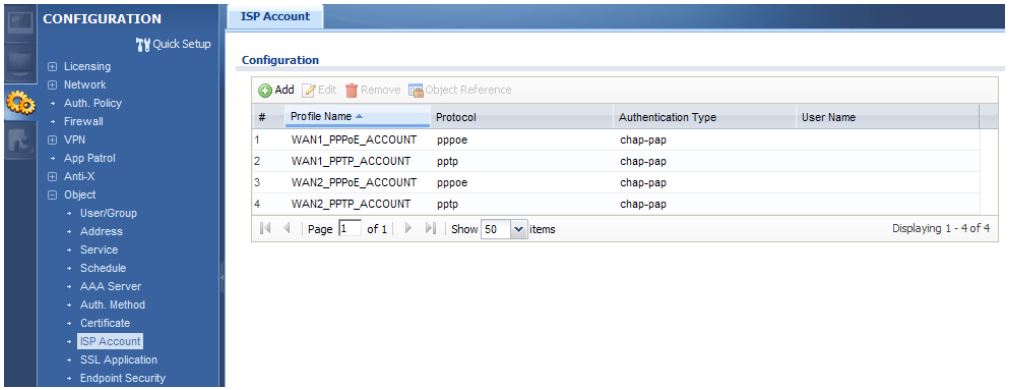
ZyWALL-5 UTM:

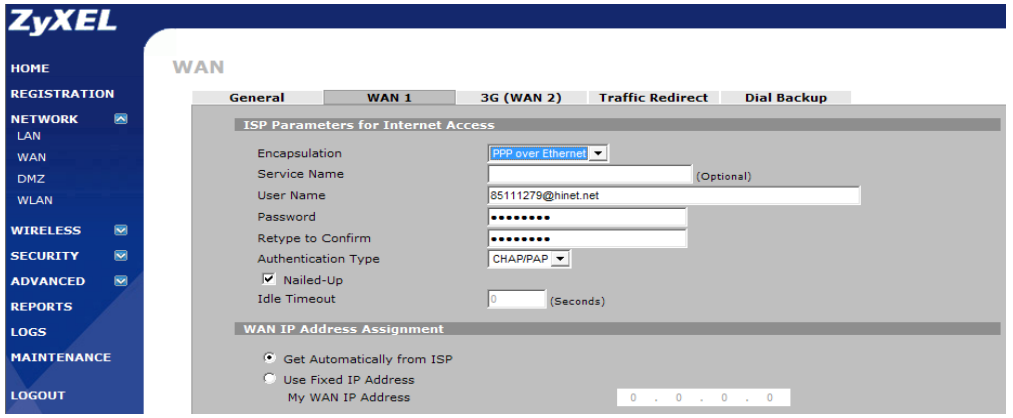
- WAN1: PPP over Ethernet
- WAN2: 3G

Goal to achieve:

Use the PPPoE interface as device's primary WAN connection and switch to the 3G interface automatically when the PPPoE interface's connection fails.

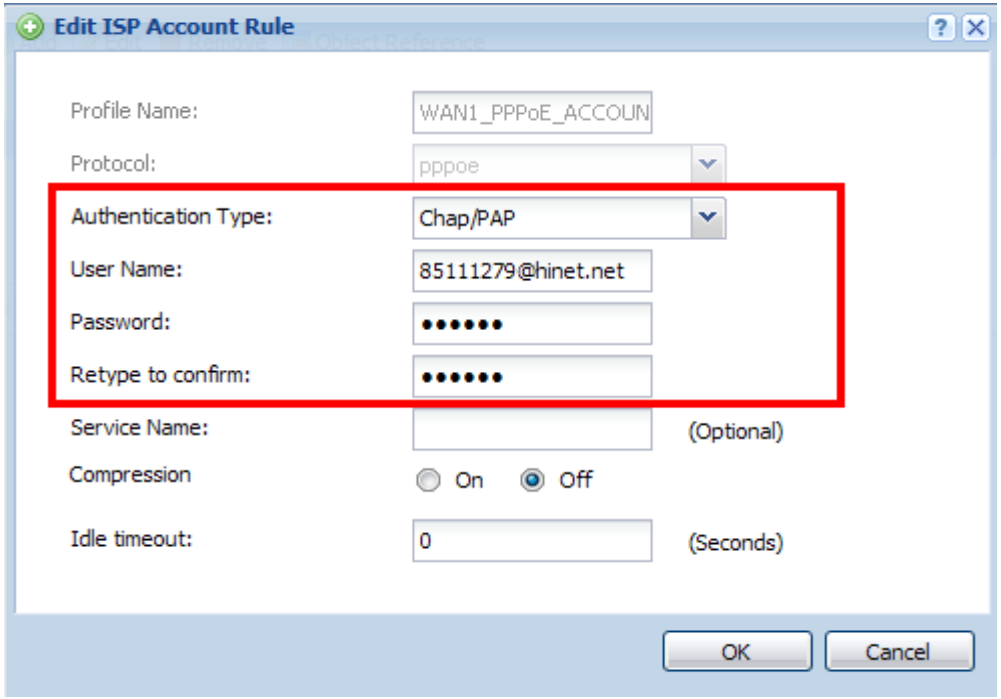
ZLD configuration	ZyNOS configuration
Step 1. Click **CONFIGURATION > Object > ISP Account** to create an ISP account first.	Step 1. Click **Network > WAN > WAN1** to open the configuration screen.



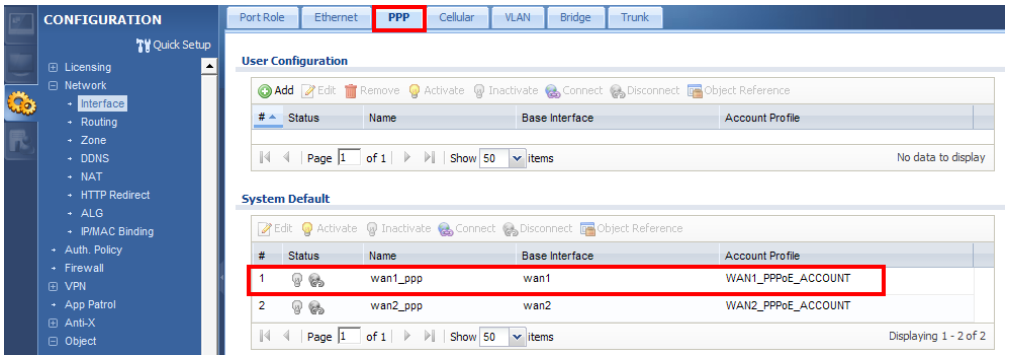


All contents copyright (c) 2010 ZyXEL Communications Corporation.

Step 2. Fill in the PPPoE user name and password.



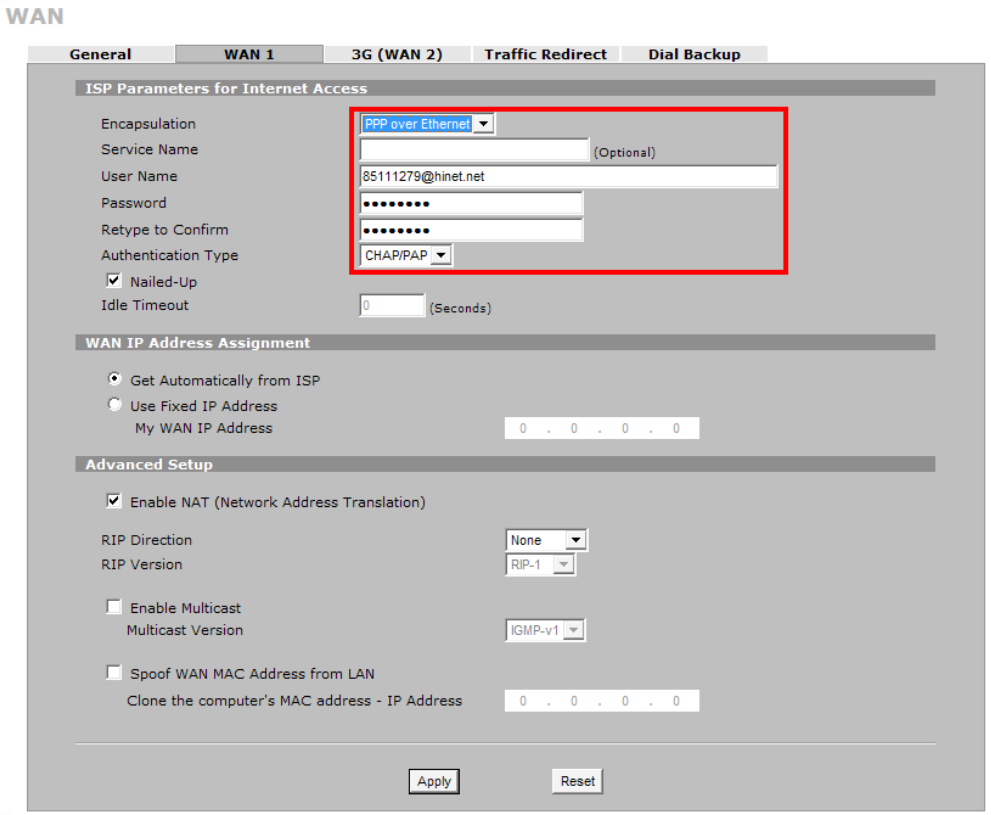
Step 3. Click **CONFIGURATION > Network > Interface > PPP** to open the configuration page. User can click the system default rule and edit it.



Step 2. Fill in the PPPoE parameters:

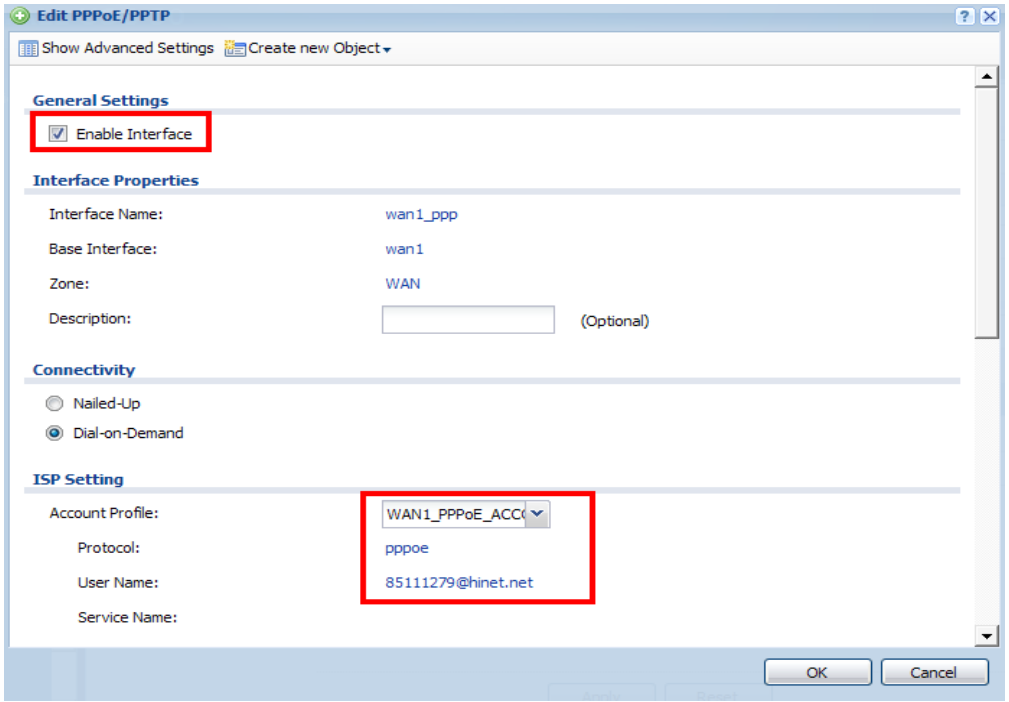
- Select **PPP over Ethernet** encapsulation mode
- User name
- Password

Step 3. Click the **Apply** button to save and apply the setting.

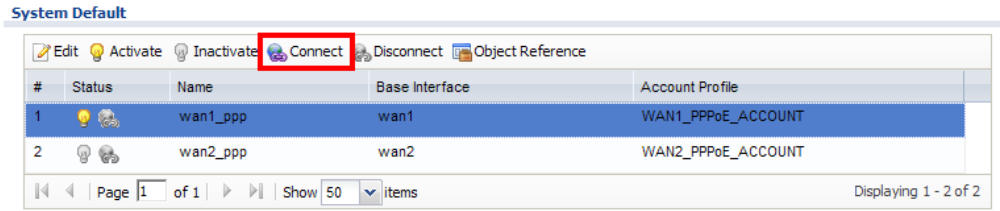


All contents copyright (c) 2010 ZyXEL Communications Corporation.

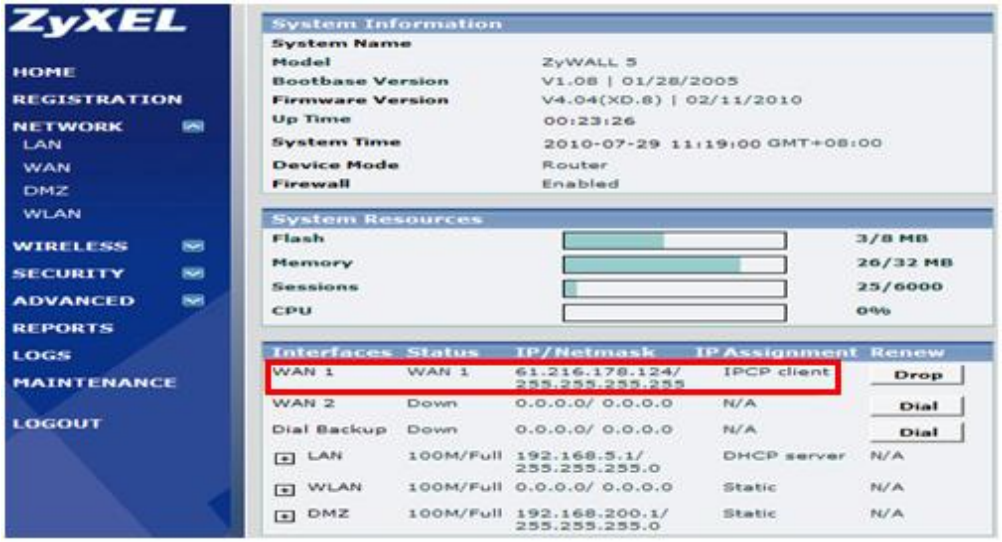
Step 4. Enable the interface and select the pre-configured ISP account to activate the PPPoE rule.



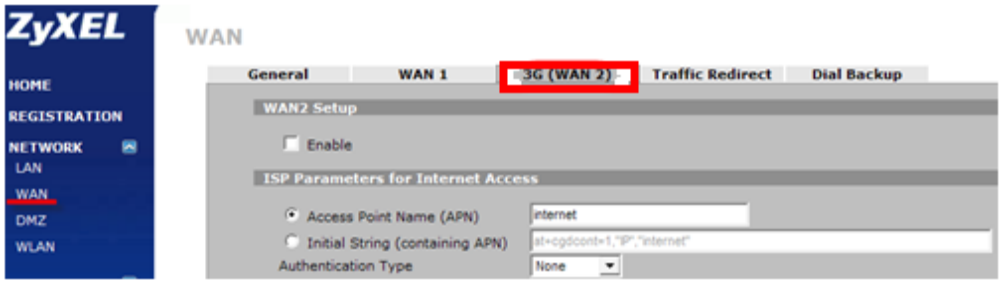
Step 5. When the configuration is done, click the **Connect** button to enable the PPPoE link. Once the connection is established, the ***connected*** icon will be displayed in front of the rule.



Step 4. Check the connection status on the dashboard.

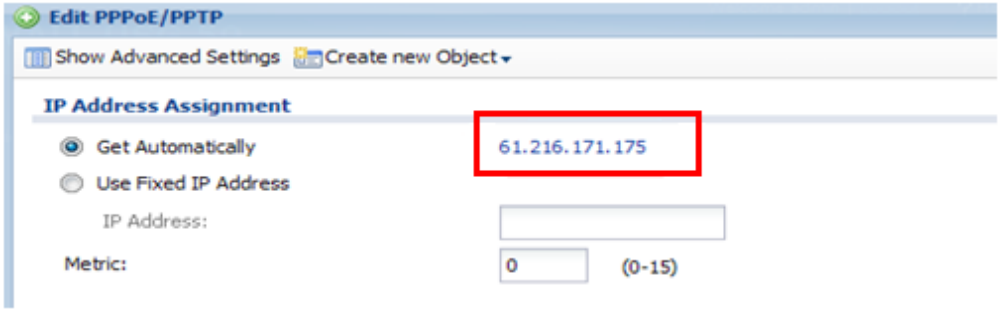


Step 5. Click **Network > WAN > 3G (WAN2)** to open the configuration screen.

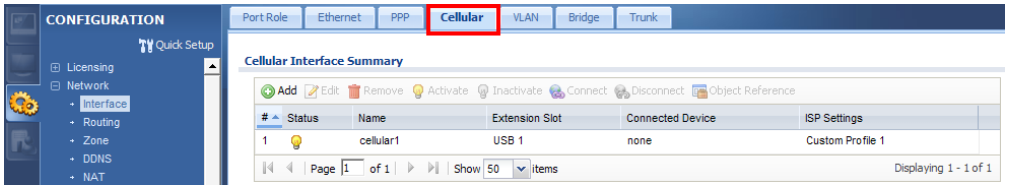


All contents copyright (c) 2010 ZyXEL Communications Corporation.

Step 6. To check the PPPoE IP address, click the PPPoE rule and check the IP address part for the information.

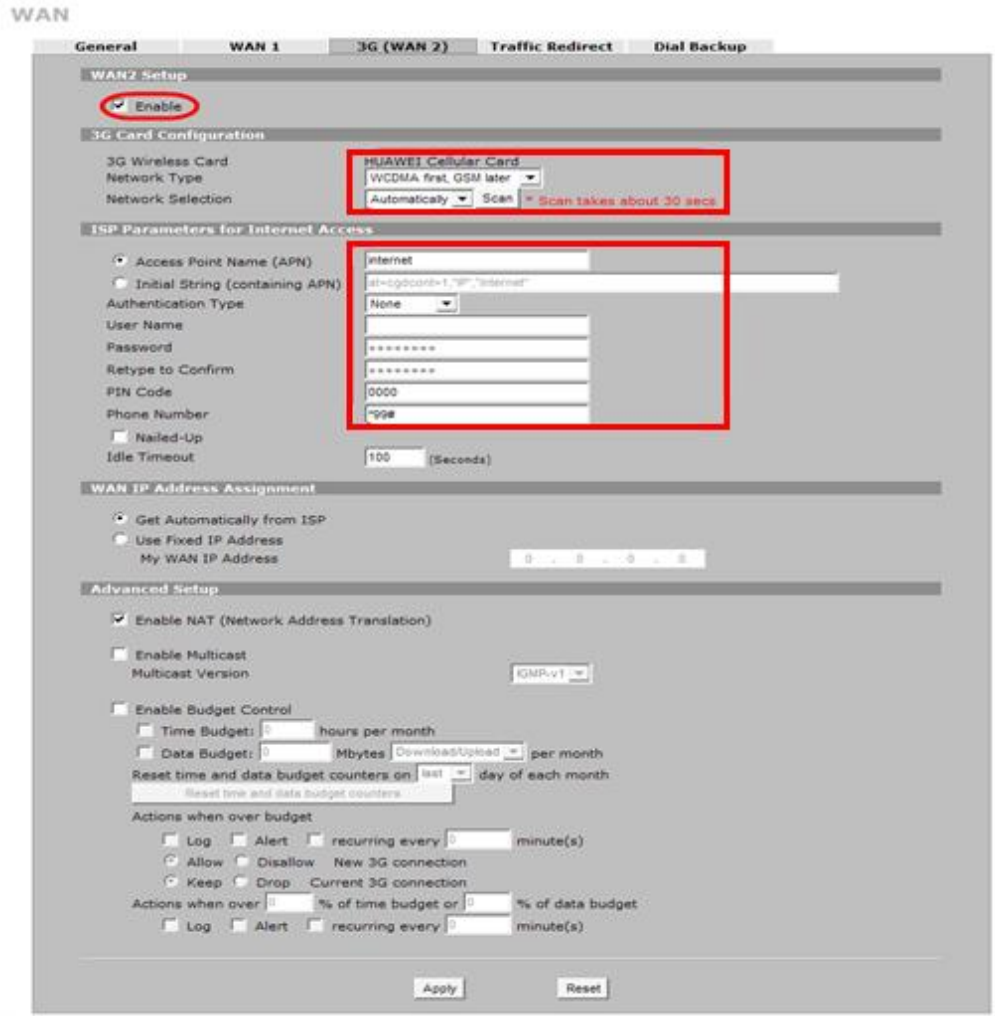


Step 7. Click **CONFIGURATION > Network > Interface > Cellular** to open the configuration page.



Step 6. Fill in the 3G connection parameters:

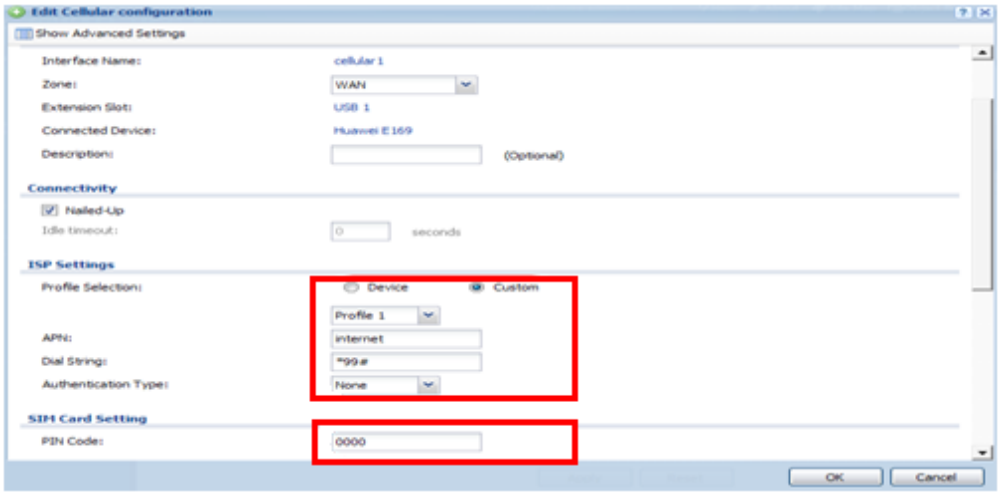
- The card information will be detected by device automatically
- Internet Access setting
  - Access Point Name (APN)
  - PIN code
  - Phone number (enter *99# if not sure what number to fill in)



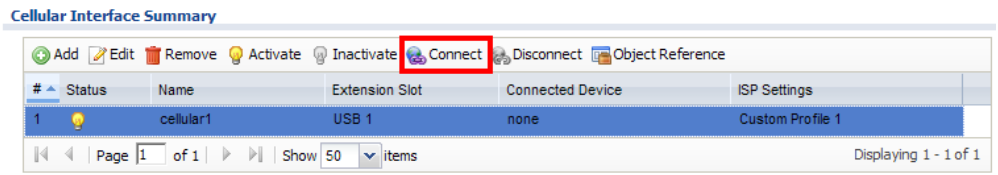
All contents copyright (c) 2010 ZyXEL Communications Corporation.

Step 8. Fill in the 3G connection parameters:

- The card information will be detected by device automatically
- ISP Settings
  - APN name
  - Dial String
- PIN code



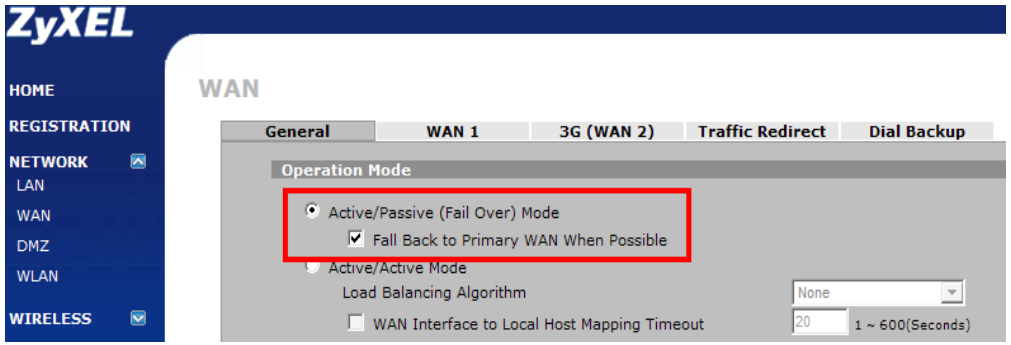
Step 9. After the configuration is done, click **Activate** to enable the rule. And then click Connect button to enable the 3G connection.



Step 7. Go to the dashboard and click the **Dial** button to trigger the rule. User can check the 3G WAN interface status to get the 3G modem detail information.

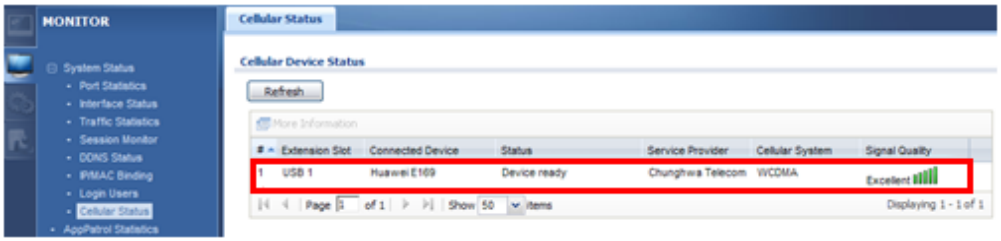
Interfaces Status IP/Netmask IP Assignment Renew
WAN 1 WAN 1 61.216.169.172/ 255.255.255.255 IPCP client Drop
WAN 2 Connected 111.82.42.186/ 255.255.255.255 IPCP client Drop
Dial Backup Down 0.0.0.0/ 0.0.0.0 N/A Dial
LAN 100M/Full 192.168.5.1/ 255.255.255.0 DHCP server N/A
WLAN 100M/Full 0.0.0.0/ 0.0.0.0 Static N/A
DMZ 100M/Full 192.168.200.1/ 255.255.255.0 Static N/A
3G WAN Interface Status hide detail...
3G Connection Status Connected (UMTS/HSDPA)
Service Provider Chunghwa Telecom
Signal Strength -67 dBm
Last Connection Up Time 0:00:30
Tx Bytes 1,389 bytes
Rx Bytes 1,719 bytes
3G Card Manufacturer HUAWEI TECHNOLOGIES CO., LTD.
3G Card Model HUAWEI E612
3G Card Firmware Revision 056.11.04.103
3G Card IMEI 356338000494116
SIM Card IMSI 466923101455327

Step 8. Now the both PPPoE and 3G connection are UP. Click on **Network > WAN > General** page to select the **Active/Passive Mode** to achieve the backup mechanism.



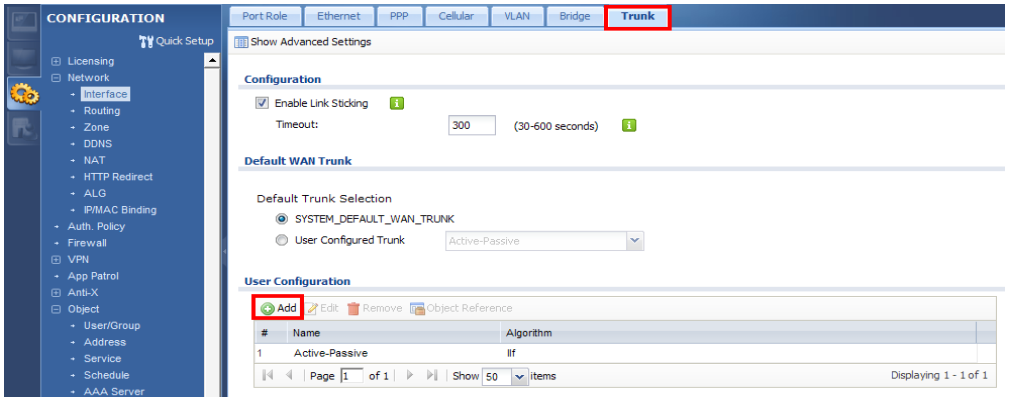
All contents copyright (c) 2010 ZyXEL Communications Corporation.

Step 10. User can check the 3G connection status on **MONITOR > System Status > Cellular Status** screen.



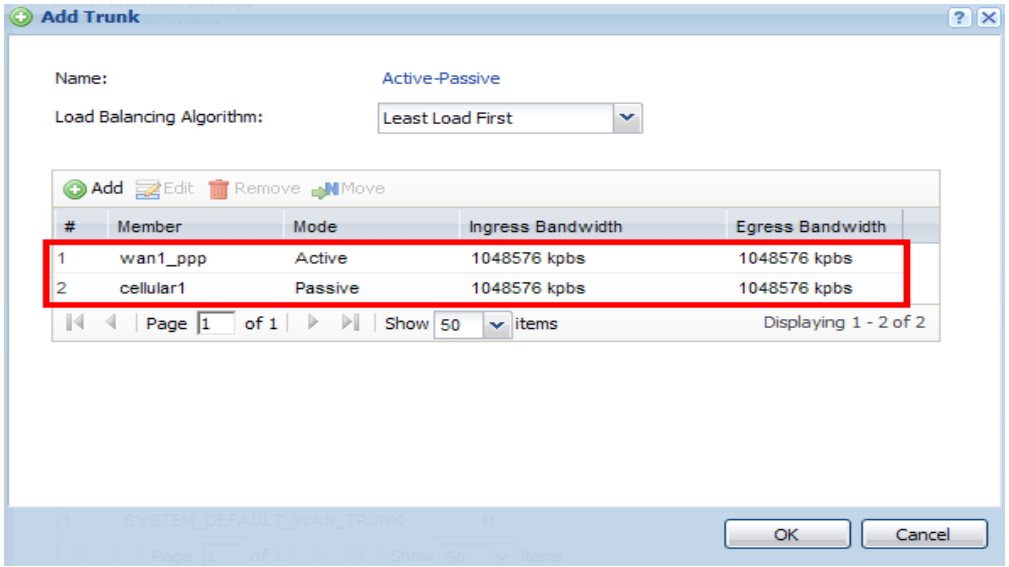
Step 11. Now both the PPPoE and 3G connection are UP. Click on **CONFIGURATION > Network > Interface > Trunk** to open the configuration screen.

Step 12. Click the **Add** button to add a User Configuration rule.

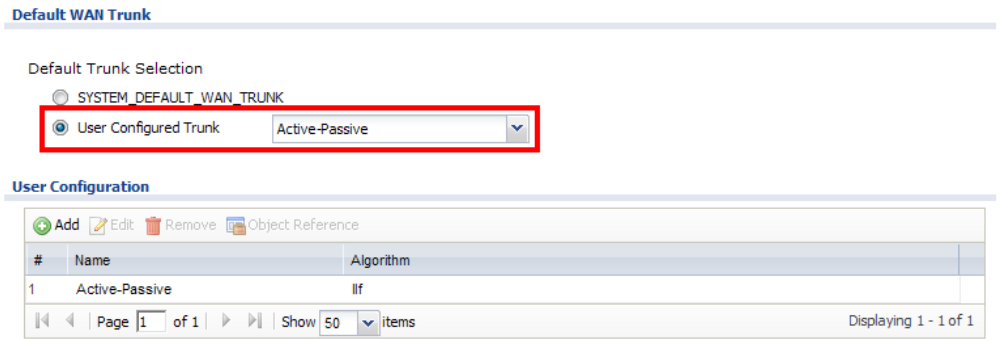


All contents copyright (c) 2010 ZyXEL Communications Corporation.

Step 13. Configure the **trunk name** and add the two interfaces: PPPoE for Active and 3G for Passive mode.



Step 14. Select the **User Configured Trunk** rule as the default WAN trunk. Then it will work using PPPoE as primary and 3G as a backup connection.



All contents copyright (c) 2010 ZyXEL Communications Corporation.

Scenario 2 — WAN Load Balancing and Customized Usage of WAN Connection for Specific Traffic

2.1 WAN Load Balancing

As an enterprise network gateway, the USG ZyWALL often has more than one WAN connection to share the company network traffic load. Without WAN load balancing, a single WAN connection may get too congested, causing the Internet traffic to become slow or even get lost.

USG ZyWALL provides network administrators with flexible ways of implementing WAN load balancing according to their demands. The outbound traffic is shared among multiple internet connections. Therefore, Internet traffic can get passed through the USG ZyWALL smoothly, improving your service quality and ensuring the Internet connections get effectively utilized.

2.1.1 Load Balancing Algorithm

WRR — Weighted Round Robin

We can assign different weights to different internet connections according to their bandwidth. The outbound traffic sessions will be sent out among the multiple WAN connections in turn; sessions will be assigned to different connections according to their proportional weights. Take the following for example:

WAN1 bandwidth: 1 Mbps.

WAN2 bandwidth: 512 Kbps.

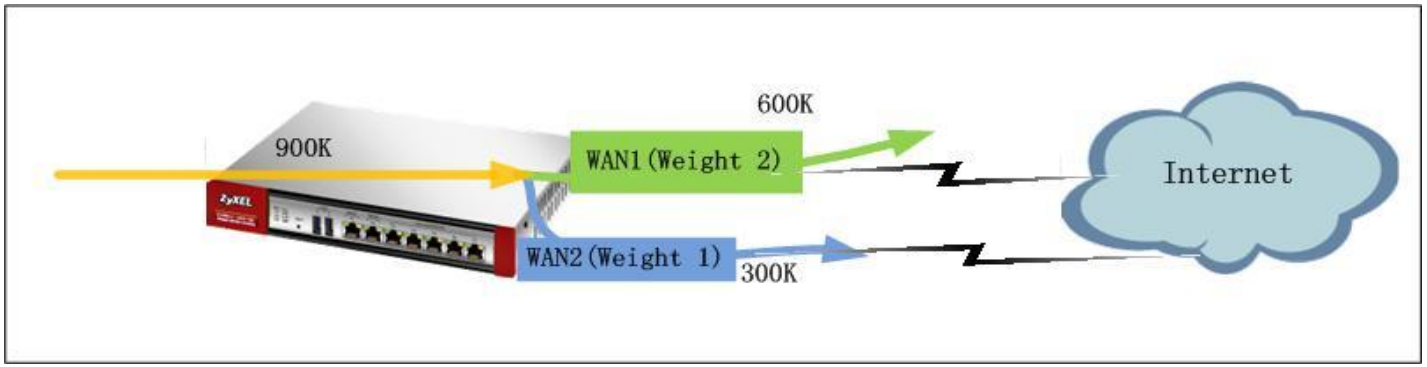
Since WAN1 has a bandwidth about twice that of WAN2, we can assign the weights to WAN1 and WAN2 as follows:

WAN1 Weight: 2

WAN2 Weight: 1

The outbound traffic sessions will be assigned to WAN1 and WAN2 according to their proportional weights. E.g., when there's total outbound traffic of 900K, 600K will be sent out over WAN1 and 300K will be sent out over WAN2.

All contents copyright (c) 2010 ZyXEL Communications Corporation.



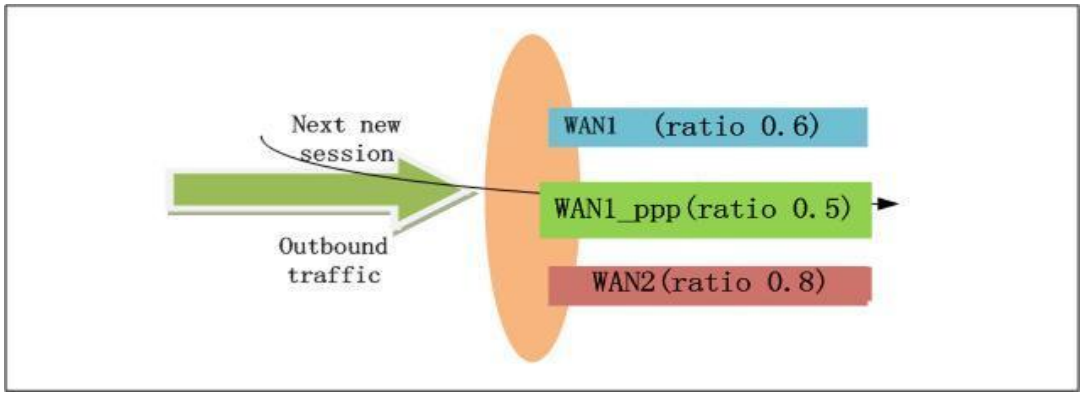
LLF — Least Load First

When choosing LLF as the load balancing algorithm, the USG will calculate each WAN interface's current outbound traffic utilization against the interface's available bandwidth. Then it will use each interface's traffic utilization ratio as the index to decide via which WAN interface it will send the next new session. The interface with the least outbound traffic utilization ratio will be used to send the next new session.

Take the following for example:

Interface	Available Bandwidth	Current measured Traffic	Utilization Ratio
WAN1	1M	600K	0.6
WAN1_ppp	512K	256K	0.5
WAN2	2M	1.6M	0.8

The next outbound new session will be sent over WAN1_ppp.



All contents copyright (c) 2010 ZyXEL Communications Corporation.

Spill-over

When choosing the Spill-over load balancing algorithm, the USG will send outbound traffic to the first interface member in the WAN trunk until its maximum allowable bandwidth is reached. Then the USG will send the excess outbound traffic to the second interface member in the WAN trunk.

This algorithm is used when the first WAN connection is free or has a lower billing rate than the second WAN connection. The company can use this load balancing algorithm to reduce Internet fees while avoiding congestion on the first WAN connection.

See the example below:

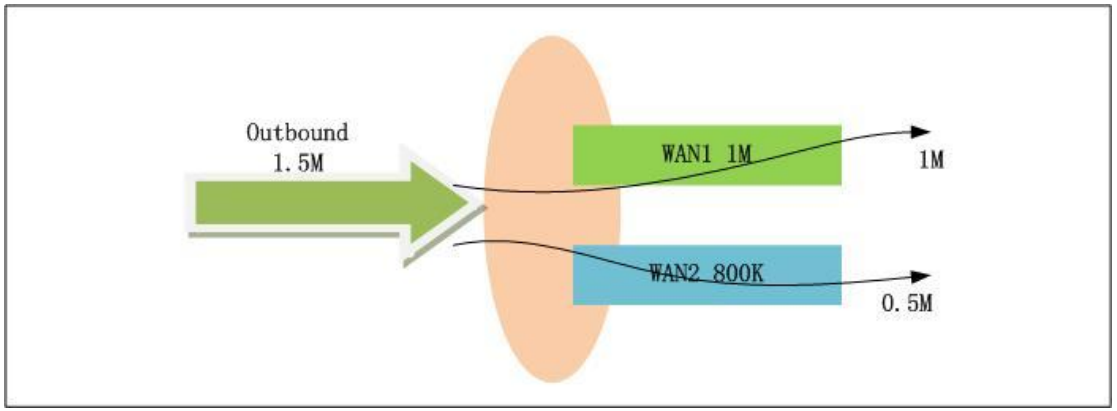
WAN1 (free connection) bandwidth: 1M

WAN2 (billing connection) bandwidth: 800K

Total outbound traffic is 1.5M. The traffic distribution among the two connections:

WAN1: 1M

WAN2: 0.5M



2.2 Customized Usage of WAN Connection for Specific Traffic Type

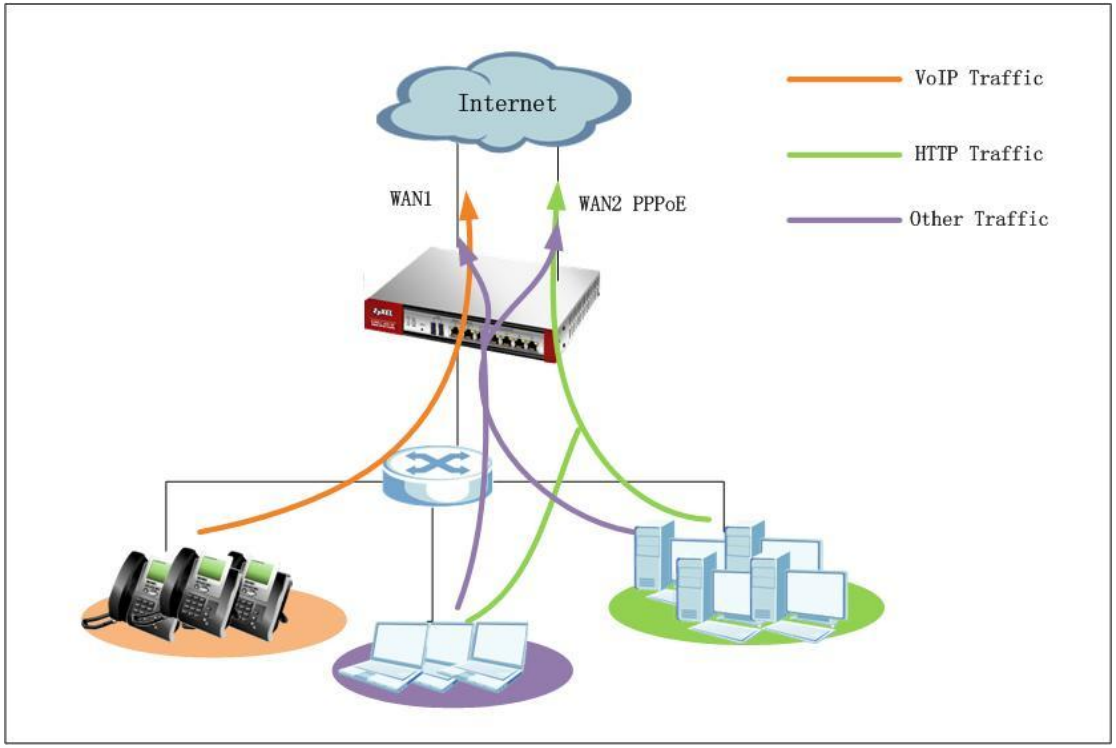
In some cases, the network administrator may prefer to send out some specific type of traffic over a specific WAN connection. For example, the ISP for WAN1 connection is also the company's ITSP (VoIP provider). Therefore, network administrator can set the gateway to send VoIP traffic out over WAN1.

Both ZyNOS ZyWALL and USG ZyWALL can achieve this application by Policy Route.

All contents copyright (c) 2010 ZyXEL Communications Corporation.

2.3 Application Scenario

The company has two WAN connections for sharing outbound internet traffic. WAN1 uses static IP, and WAN2 uses a PPPoE connection. Since WAN1 ISP is also the company's VoIP provider, the network administrator wants VoIP traffic primarily sent out over WAN1. In case WAN1 is down, the VoIP traffic can still go out over WAN2 PPPoE connection. Network administrator also wants HTTP traffic sent over WAN2 PPPoE connection primarily. In case WAN2 PPPoE is down, LAN users can still surf internet over WAN1. For all other types of traffic, administrator needs the two WAN connections to share the outbound traffic load, performing load balancing.



All contents copyright (c) 2010 ZyXEL Communications Corporation.

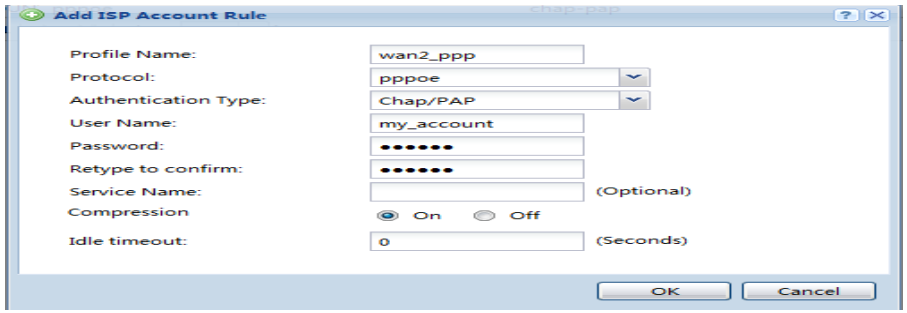
2.4 Configuration Guide

Network Conditions:

- LAN subnet: 192.168.1.0/24
- WAN1 IP: 200.0.0.1
- WAN2 PPPoE IP: Dynamic
- WAN1 download bandwidth: 2M
- WAN2 download bandwidth: 2M

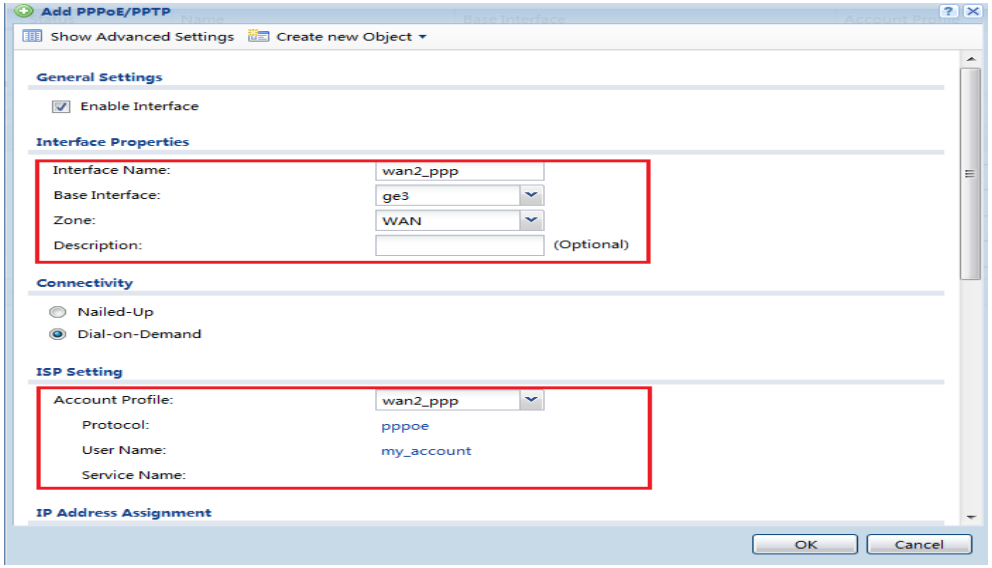
Goals to achieve:

1) VoIP traffic goes out primarily through WAN1. In case WAN1 is down, it will go out via WAN2 PPPoE connection.
2) HTTP traffic goes out primarily through WAN2 PPPoE connection. In case WAN2 PPPoE is down, it will go out via WAN1.
3) All other traffic goes out via WAN trunk performing Load Balancing with Least Load Balancing algorithm.

ZLD configuration	ZyNOS configuration
Step 1. Configure a PPPoE account on WAN2 interface. a. Go to **CONFIGURATION > Object > ISP Account,** add a PPPoE account:  	Step 1. Go to **Advanced > Policy Route**, add policy route to route VoIP traffic out primarily from WAN1, and WAN2 as backup. **Criteria:** **Application:** SIP **Source:** Choose LAN interface. Address range: 192.168.1.0~192.168.1.255 **Destination:** Any. **Action Applies to:** Matched packets. **Routing Action**:

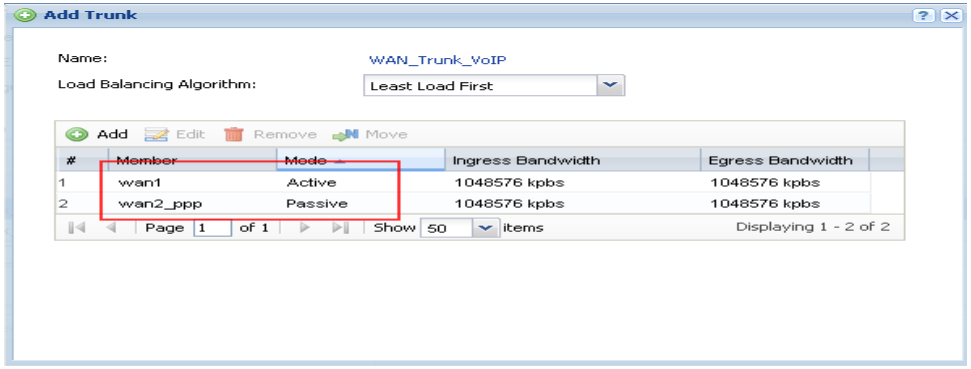
All contents copyright (c) 2010 ZyXEL Communications Corporation.

b. Go to **CONFIGURATION > Network > Interface > PPP**, add a new PPP interface which is based on WAN 2(ge3) interface:

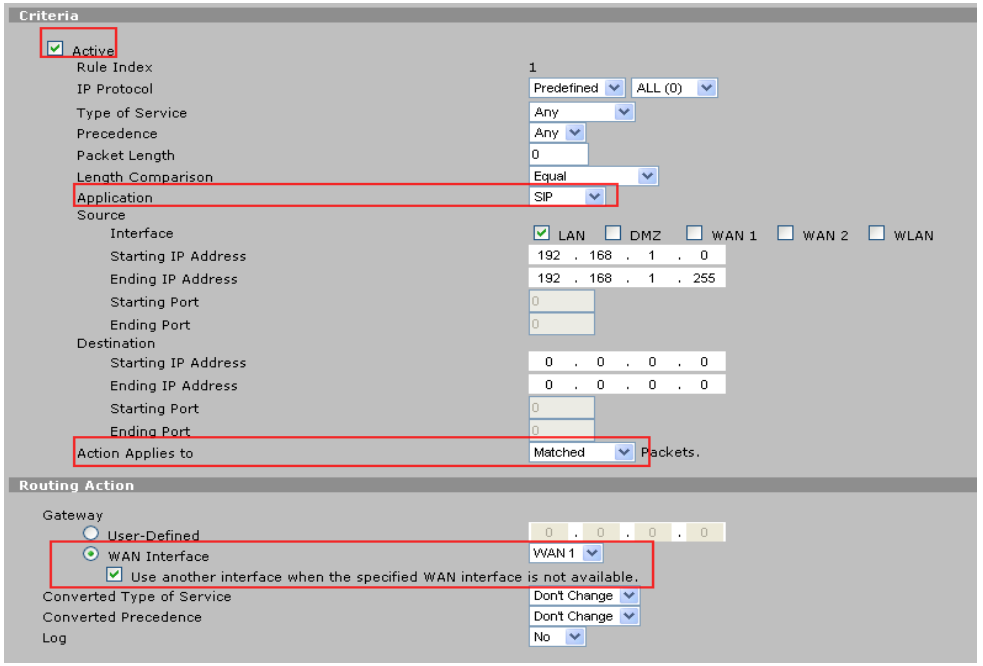


Step 2. Go to **CONFIGURATION > Network > Interface > Trunk**. Add WAN Trunks.

a. Add WAN trunk for VoIP traffic — Set WAN1 as Active mode, while setting WAN2_ppp as Passive mode.

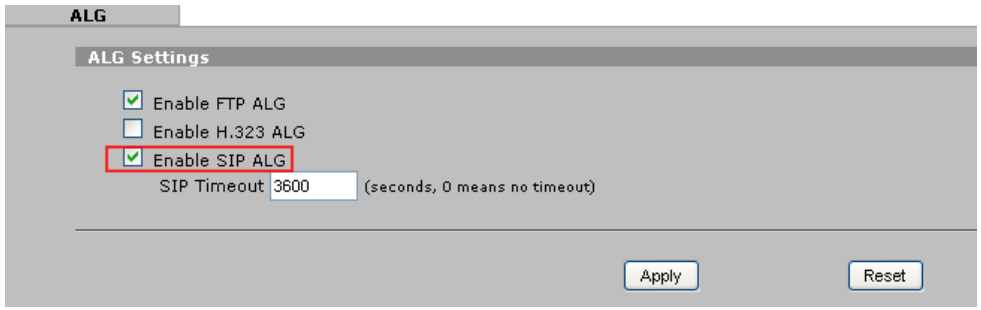


Choose WAN interface WAN1, and enable **Use another interface when the specified WAN interface is not available**.


Criteria
Active
Rule Index 1
IP Protocol Predefined ALL (0)
Type of Service Any
Precedence Any
Packet Length 0
Length Comparison Equal
Application SIP
Source
Interface LAN DMZ WAN 1 WAN 2 WLAN
Starting IP Address 192 . 168 . 1 . 0
Ending IP Address 192 . 168 . 1 . 255
Starting Port
Ending Port
Destination
Starting IP Address 0 . 0 . 0 . 0
Ending IP Address 0 . 0 . 0 . 0
Starting Port
Ending Port
Action Applies to Matched Packets.
Routing Action
Gateway
User-Defined
WAN Interface WAN 1
Use another interface when the specified WAN interface is not available.
Converted Type of Service Don't Change
Converted Precedence Don't Change
Log No

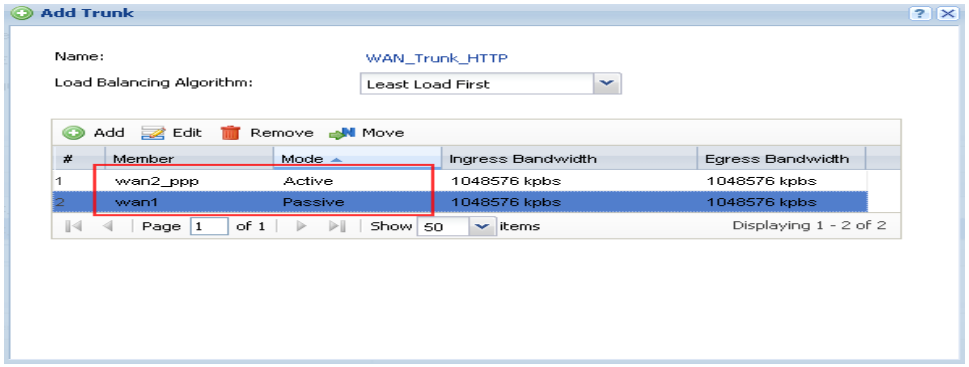
Please enable **SIP ALG** to let this policy route apply to all VoIP traffic including both SIP signaling and RTP (voice data).

Go to **Advanced > ALG**, enable SIP ALG.

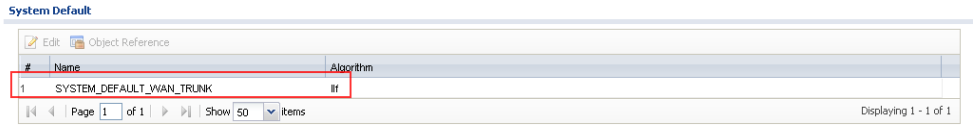


All contents copyright (c) 2010 ZyXEL Communications Corporation.

b. Add WAN trunk for HTTP traffic — Set WAN2_ppp as Active mode, while setting WAN1 as Passive mode.



c. Use **SYSTEM_DEFAULT_WAN_TRUNK** to do load balancing for all other traffic.



Step 2. Go to **Advanced > Policy Route**, add a policy route to route HTTP traffic out primarily through WAN2, leaving WAN1 as backup.

Criteria:

IP Protocol: TCP (6)

Application: Custom

Source IP: Choose interface LAN. Address range: 192.168.1.0~192.168.1.255

Source port: Any

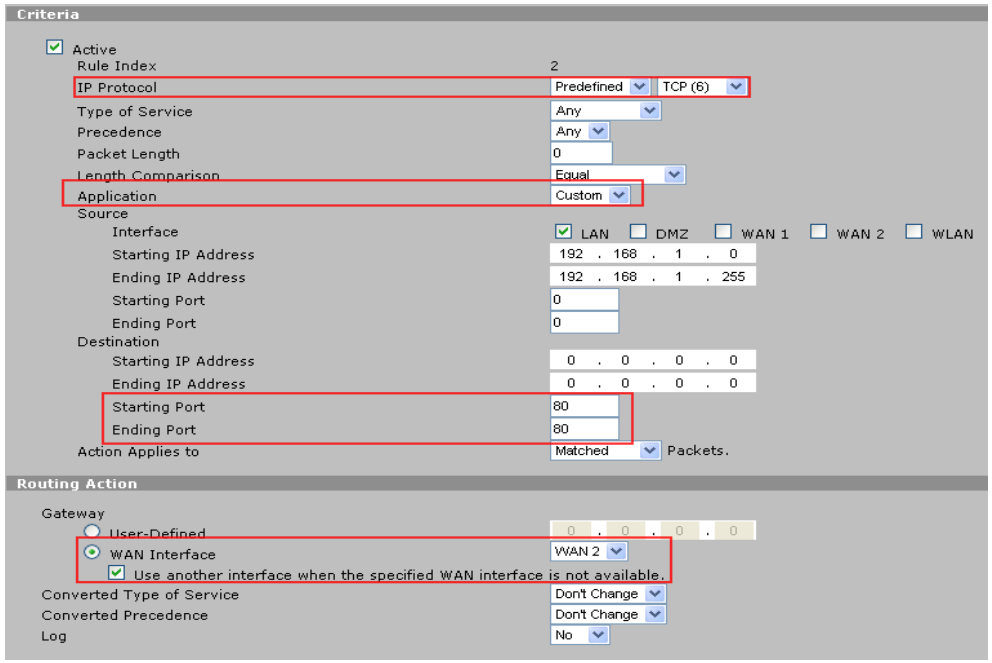
Destination IP: Any

Destination Port: 80

Action Applies to: Matched packets.

Routing Action:

Choose WAN interface WAN2, and enable **Use another interface when the specified WAN interface is not available**.


Criteria
Active
Rule Index 2
IP Protocol Predefined TCP (6)
Type of Service Any
Precedence Any
Packet Length 0
Length Comparison Equal
Application Custom
Source
Interface LAN DMZ WAN 1 WAN 2 WLAN
Starting IP Address 192 . 168 . 1 . 0
Ending IP Address 192 . 168 . 1 . 255
Starting Port 0
Ending Port 0
Destination
Starting IP Address 0 . 0 . 0 . 0
Ending IP Address 0 . 0 . 0 . 0
Starting Port 80
Ending Port 80
Action Applies to Matched Packets.
Routing Action
Gateway
User-Defined 0 . 0 . 0 . 0
WAN Interface WAN 2
Use another interface when the specified WAN interface is not available.
Converted Type of Service Don't Change
Converted Precedence Don't Change
Log No

All contents copyright (c) 2010 ZyXEL Communications Corporation.

Step 3. Go to **CONFIGURATION > Network > Routing > Policy Route**, add policy routes for VoIP traffic and HTTP traffic.

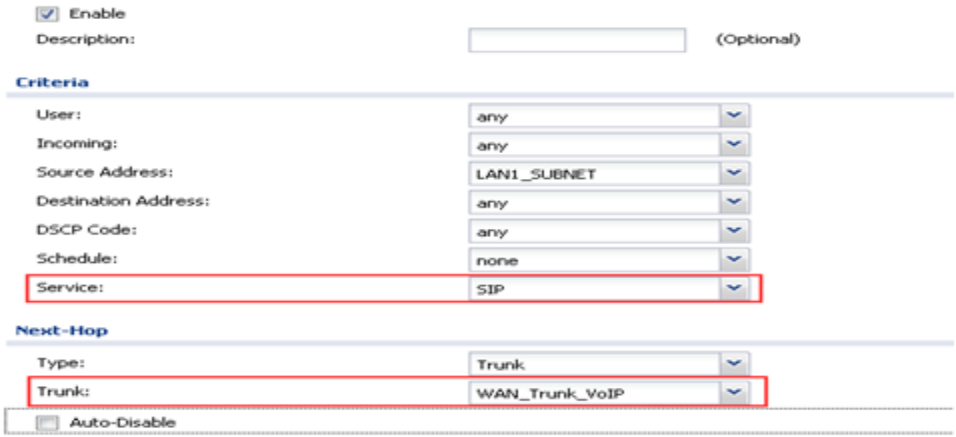
a. Add a policy route for VoIP traffic:

Source: LAN1_subnet

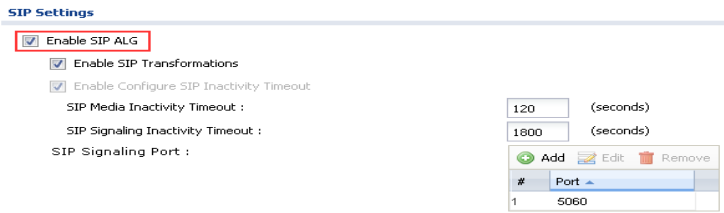
Destination: Any

Service: SIP

Next Hop: select the newly created WAN trunk WAN_Trunk_VoIP



Please note that to make sure this policy route applies to all VoIP traffic, including both the SIP signaling and RTP (voice data), we need to enable **SIP ALG**. Go to **Configuration > Network > ALG**, enable SIP ALG.



Step 3. For all other traffic, we use the two WAN connections to perform load balancing. Go to **Network > WAN > General**.

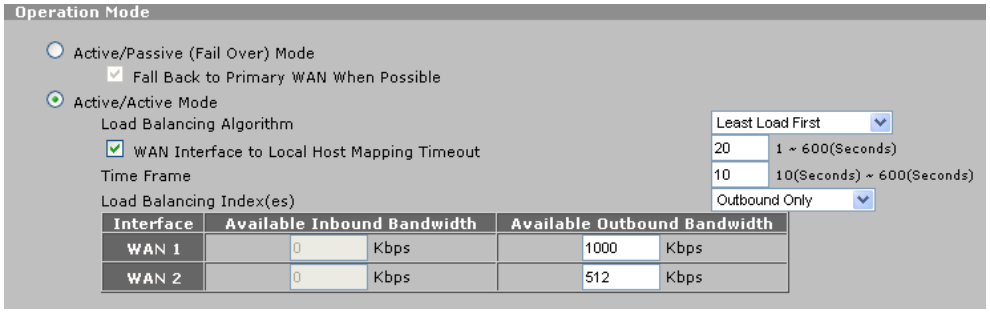
Choose Active/Active Mode.

Set the **Load Balancing Algorithm** to Least Load First.

To avoid the situation where traffic from the same LAN host may be sent over different WAN interfaces, which may cause servers to refuse the connection due to a different source IP, we enable and set "**WAN Interface to Local Host Mapping Timeout**" to a specific time period.

For Load Balancing Index (es), we choose **Outbound Only**.

Set the available outbound bandwidth for the two WAN connections according to the bandwidth obtained from each ISP.



All contents copyright (c) 2010 ZyXEL Communications Corporation.

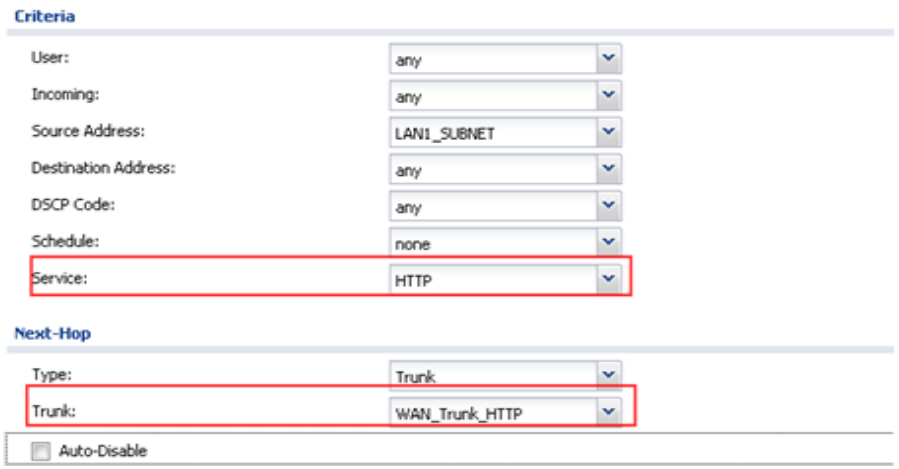
b. Add a policy route for HTTP traffic:

Source: LAN1_subnet

Destination: Any

Service: HTTP

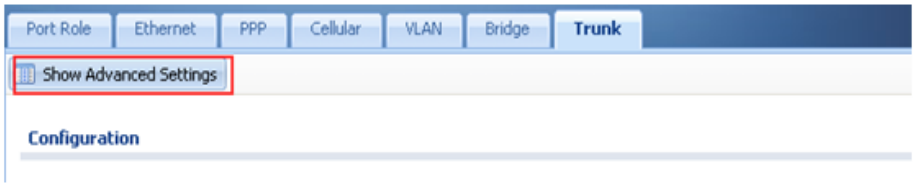
Next Hop: Select the newly created WAN trunk WAN_Trunk_HTTP.



All contents copyright (c) 2010 ZyXEL Communications Corporation.

c. For all other traffic, use **SYSTEM_DEFAULT_WAN_TRUNK** to do load balancing.

Go to **Configuration > Network > Interface > Trunk.** Click Show Advanced Settings.



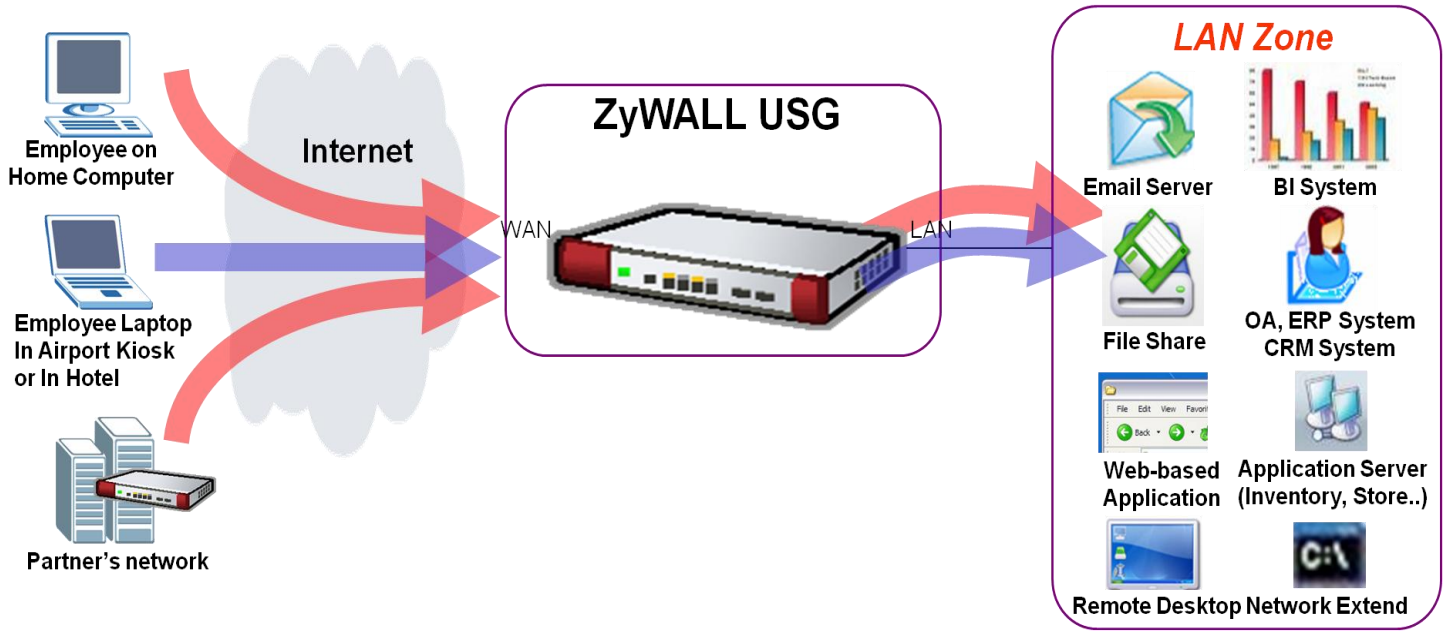
Make sure **Default SNAT** is enabled. Select **SYSTEM_DEFAULT_WAN_TRUNK** in Default Trunk Selection.

All contents copyright (c) 2010 ZyXEL Communications Corporation.

Scenario 3 — How to configure NAT if you have Internet-facing public servers

3.1 Application Scenario

It is a common practice to place company servers behind the USG's protection; while at the same time letting WAN side clients/servers access the intranet servers. To give an example, the company may have an internal FTP server, which needs to be accessible from the Internet as well. To fulfill this requirement, user can configure a NAT mapping rule to forward the traffic from Internet side to intranet side. This feature can not only ensure service availability but also helps avoid exposing the server's real IP address to be attacked.



All contents copyright (c) 2010 ZyXEL Communications Corporation.

3.2 Configuration Guide

Network Conditions:

USG-50:

- WAN IP: 59.124.163.152
- FTP server IP:192.168.50.33

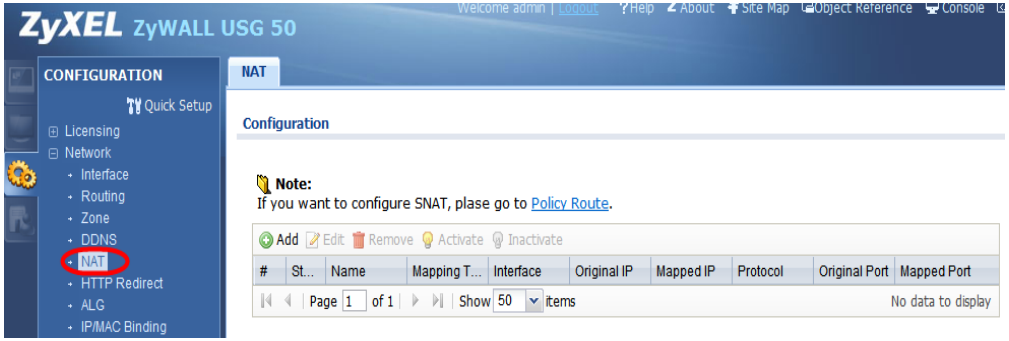
ZyWALL-5 UTM:

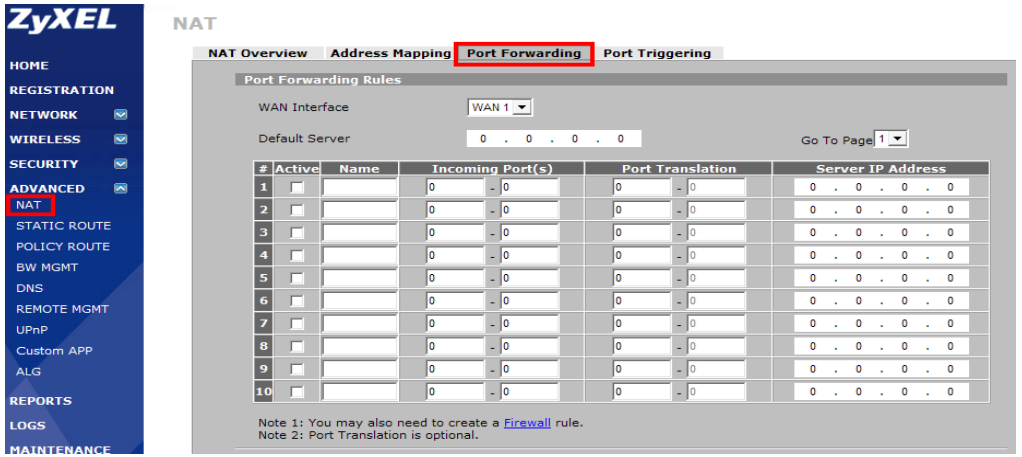
- WAN IP: 10.59.1.50
- FTP server IP: 192.168.5.33

Goal to achieve:

User Tom can access the internal FTP server by accessing the Internet-facing WAN IP address.

ZLD configuration	ZyNOS configuration
Step 1. Click **CONFIGURATION > Network > NAT** to open the configuration screen.	Step 1. Click **ADVANCED > NAT > Port Forward**ing to open the configuration screen.



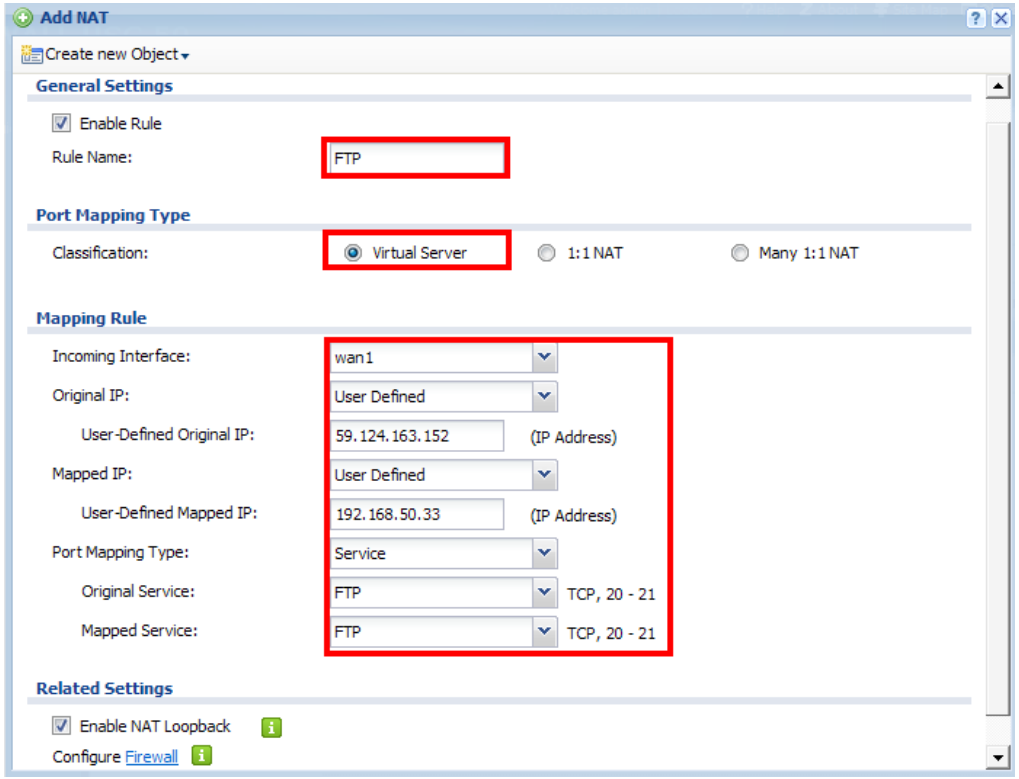


All contents copyright (c) 2010 ZyXEL Communications Corporation.

Step 2. Click the **Add** button to create a mapping rule.

Step 3. In this page user needs to configure:

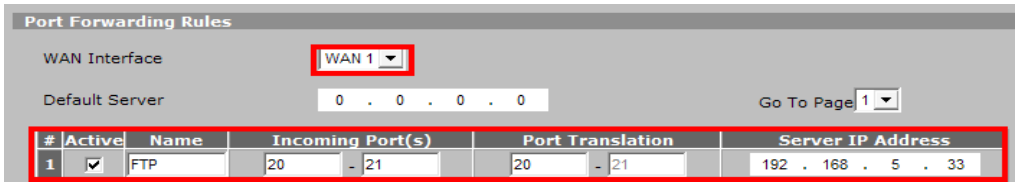
- Rule's name
- Select Virtual Server type to let USG-50 do packet forwarding
- Fill in the **Original IP** (WAN IP) address
- Fill in the **Mapped IP** (Internal FTP server IP) address
- Select the **service to be mapped** (FTP); the ports will be selected automatically



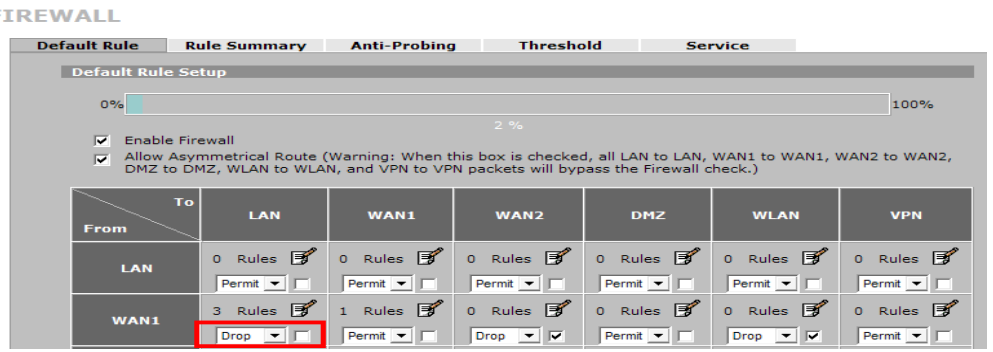
Step 2. Configure the mapping rule. User needs to select the WAN interface for the incoming access, choosing the WAN IP for users to access.

Step 3. Then configure the incoming ports, translation ports and the internal FTP server IP address.

In this case, when the user accesses the WAN IP address with the port 20/21, the ZyWALL-5 UTM will forward the request to the FTP server, 192.168.5.33, with the port 20/21. Thus, user can access the internal FTP server without problem.


Port Forwarding Rules
WAN Interface
WAN 1
Default Server
0 . 0 . 0 . 0
Go To Page 1
Active Name Incoming Port(s) Port Translation Server IP Address
1 FTP 20 - 21 20 - 21 192 . 168 . 5 . 33

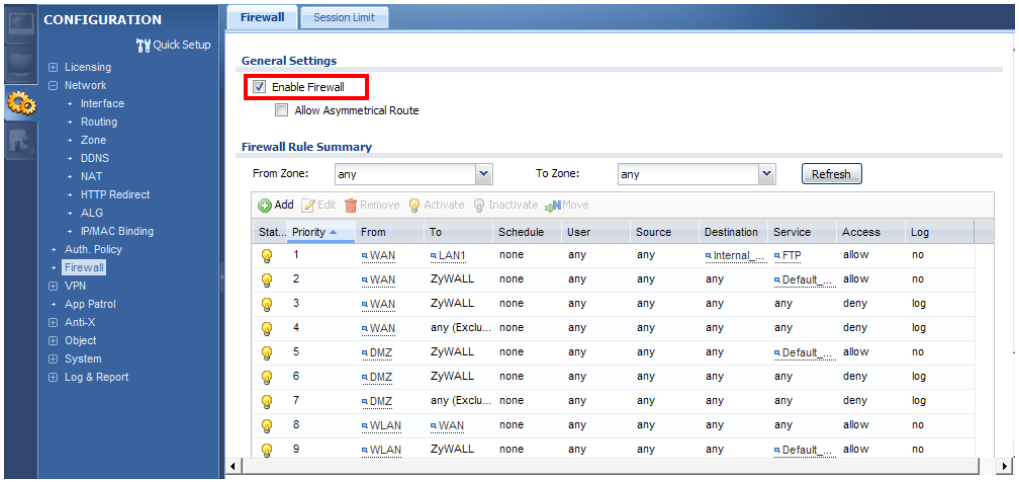
Step 4. The port forwarding rule enables delivery of the access request from WAN to the internal network, but the user still needs to configure access privileges by adjusting the firewall rule. By default all WAN to LAN access is dropped.



All contents copyright (c) 2010 ZyXEL Communications Corporation.

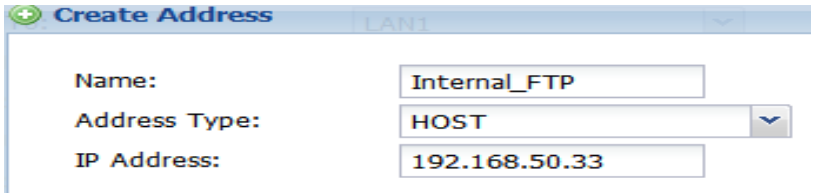
Step 4. Click **CONFIGURATION > Network > Firewall** to open the firewall configuration screen.

Here assume the user already assigned the WAN interface to WAN zone and LAN interface to LAN1 zone.

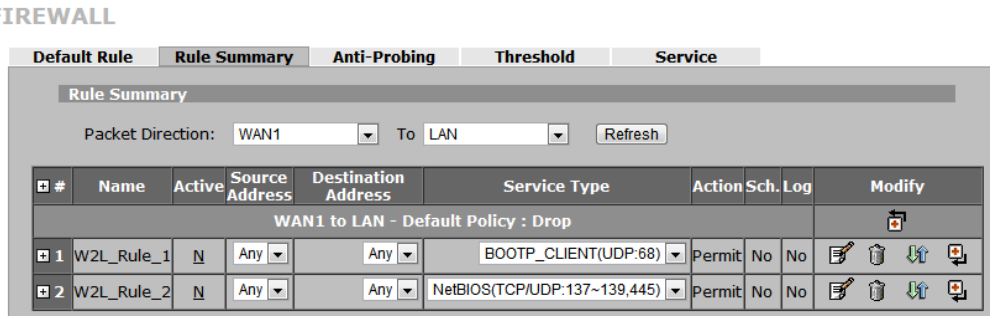


Step 5. Click the Add button to create a firewall rule to enable the FTP service to pass from WAN to LAN1.

Step 6. User can create an address object for the internal FTP server for further configuration usage. Click **Create new Object** for this function.



Step 5. Click **Rule Summary** to customize the setup. The default is to drop all packets.


FIREWALL
Default Rule
Rule Summary
Anti-Probing
Threshold
Service
Rule Summary
Packet Direction: WAN1 To LAN Refresh
Name Active Source Address Destination Address Service Type Action Sch. Log Modify
WAN1 to LAN - Default Policy : Drop
1 W2L_Rule_1 N Any Any BOOTP_CLIENT(UDP:68) Permit No No
2 W2L_Rule_2 N Any Any NetBIOS(TCP/UDP:137~139,445) Permit No No

Step 6. Configure the firewall rule to enable the FTP service to pass from WAN1 to LAN.

- **Source IP address** is not specific
- **Destination IP address** is the FTP server's address
- Select **FTP service** (with port 20/21) to be enabled
- Select the **Permit** action for matched packets

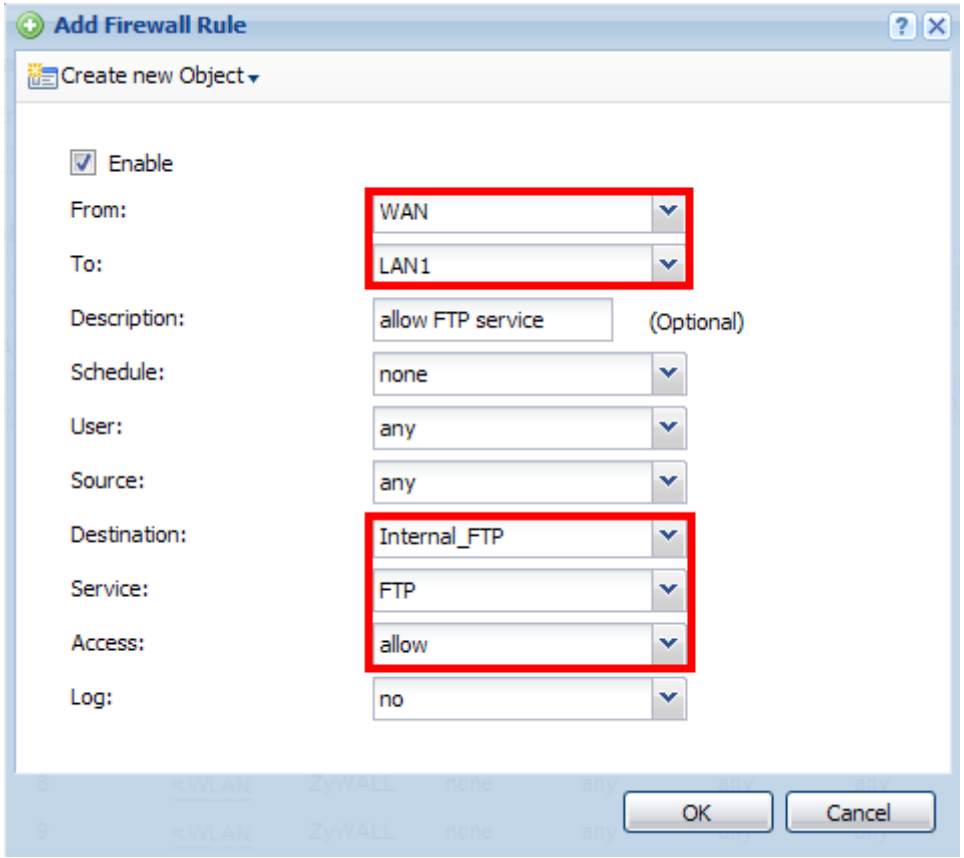
After this configuration, user can access the FTP server from WAN side.

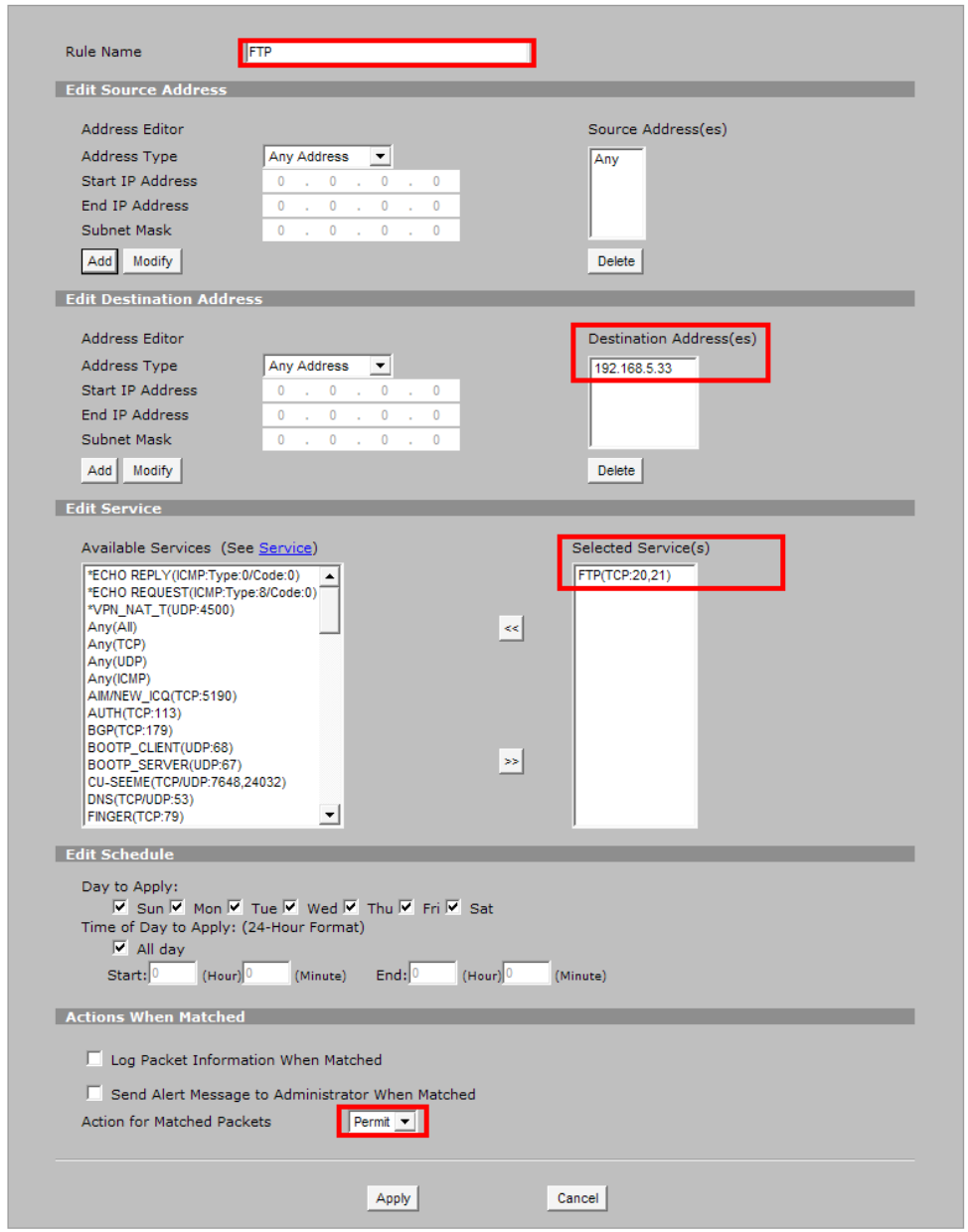
All contents copyright (c) 2010 ZyXEL Communications Corporation.

Step 7. Configure the rule to:

- **Allow access** from WAN to LAN1
- **Source IP address** is not specific
- **Destination IP address** is the FTP server's address
- Select **FTP service** (with port 20/21) to be enabled
- Select the **allow** action for matched packets

After this configuration, user can access the FTP server from WAN side.





All contents copyright (c) 2010 ZyXEL Communications Corporation.

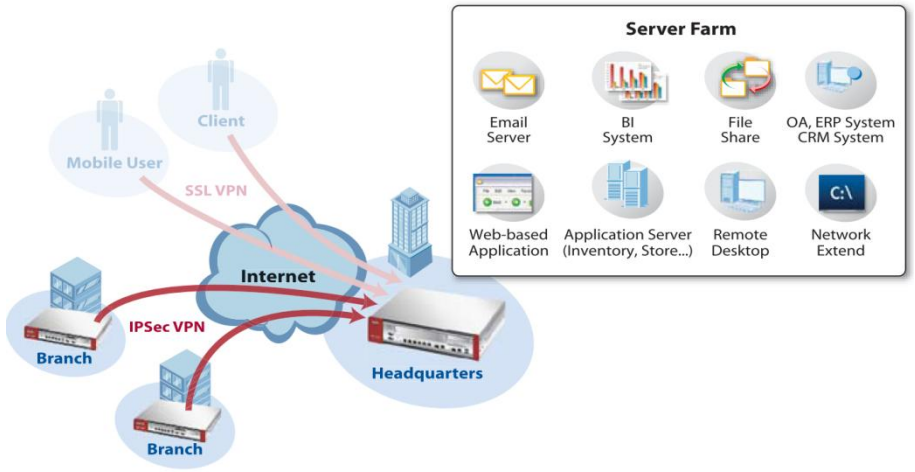
Scenario 4 — Secure site-to-site connections using IPSec VPN

4.1 Application Scenario

A virtual private network (VPN) provides secure communications between sites without the expense of leased site-to-site lines. A secure VPN is a combination of tunneling, encryption, authentication, access control and auditing. It is used to transport traffic over the Internet or any insecure network that uses TCP/IP for communication.

Internet Protocol Security (IPSec) offers standards-based VPN solutions that enable flexible scenarios for secure data communications across a public network like the Internet. An IPSec VPN tunnel is usually established in two phases. Each phase establishes a security association (SA), a contract indicating what security parameters the ZyWALL and the remote IPSec router will use. The first phase establishes an Internet Key Exchange (IKE) SA between the ZyWALL and a remote IPSec router. The second phase uses the IKE SA to securely establish an IPSec SA through which the ZyWALL and remote IPSec router can send data between computers on the local network and remote network.

The USG can provide secure site-to-site access between remote locations and corporate resources through the Internet. Using IPSec VPN, companies can secure connections to branch offices, partners and headquarters as the illustration below.



All contents copyright (c) 2010 ZyXEL Communications Corporation.

4.2 Configuration Guide

Network Conditions:

USG-50:

- WAN IP: 59.124.163.152
- Local subnet: 192.168.50.0/24

ZyWALL-5 UTM:

- WAN IP: 10.59.1.50
- Local subnet: 192.168.5.0/24

IPSec VPN Conditions:

Phase 1:

- Authentication: 1234567890
- Local/Peer ID type: IP 0.0.0.0
- Negotiation: Main mode
- Encryption Algorithm: 3DES
- Authentication Algorithm: MD5
- Key Group: DH1

Phase 2:

- Encapsulation Mode: Tunnel
- Active Protocol: ESP
- Encryption Algorithm: DES
- Authentication Algorithm: SHA1
- Perfect Forward Secrecy: None

Goal to achieve:

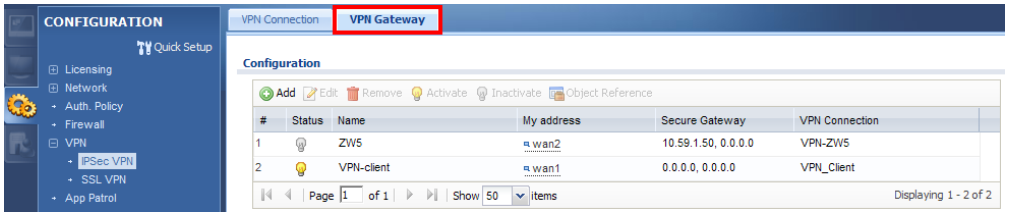
Build up the IPSec VPN tunnel between USG-50 and ZyWALL-5 UTM with the above configuration.

All contents copyright (c) 2010 ZyXEL Communications Corporation.

ZLD configuration

Step 1. Click **CONFIGURATION > VPN > IPSec VPN > VPN Gateway** to open the configuration screen.

Step 2. Click the **Add** button to add a VPN gateway rule.



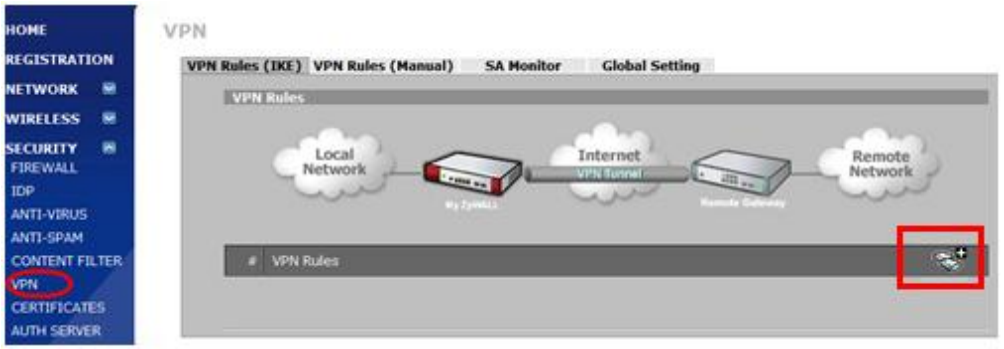
Step 3. To configure the VPN gateway rule, user needs to fill in:

- VPN gateway name
- Gateway address; both local (My Address) and peer (Peer GW Address)
- Authentication setting
  - Pre-Shared Key
  - ID Type setting (Local and Peer side)
- Phase-1 setting
  - Negotiation mode
  - Encryption algorithm
  - Authentication algorithm
  - Key Group

ZyNOS configuration

Step 1. Click **SECURITY > VPN > VPN RULES (IKE)** to open the configuration screen.

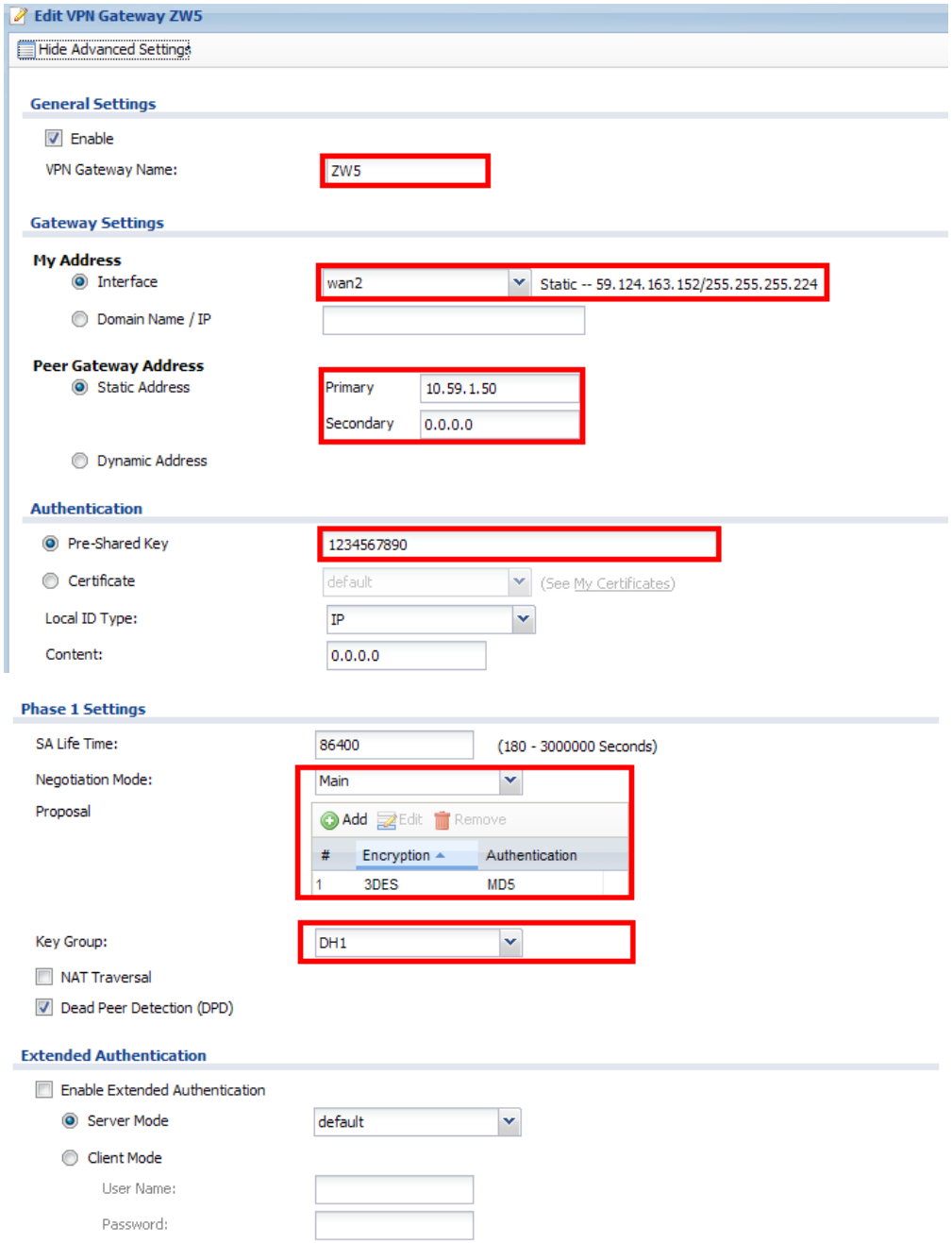
Step 2. Click the **Add** button to add a gateway policy.

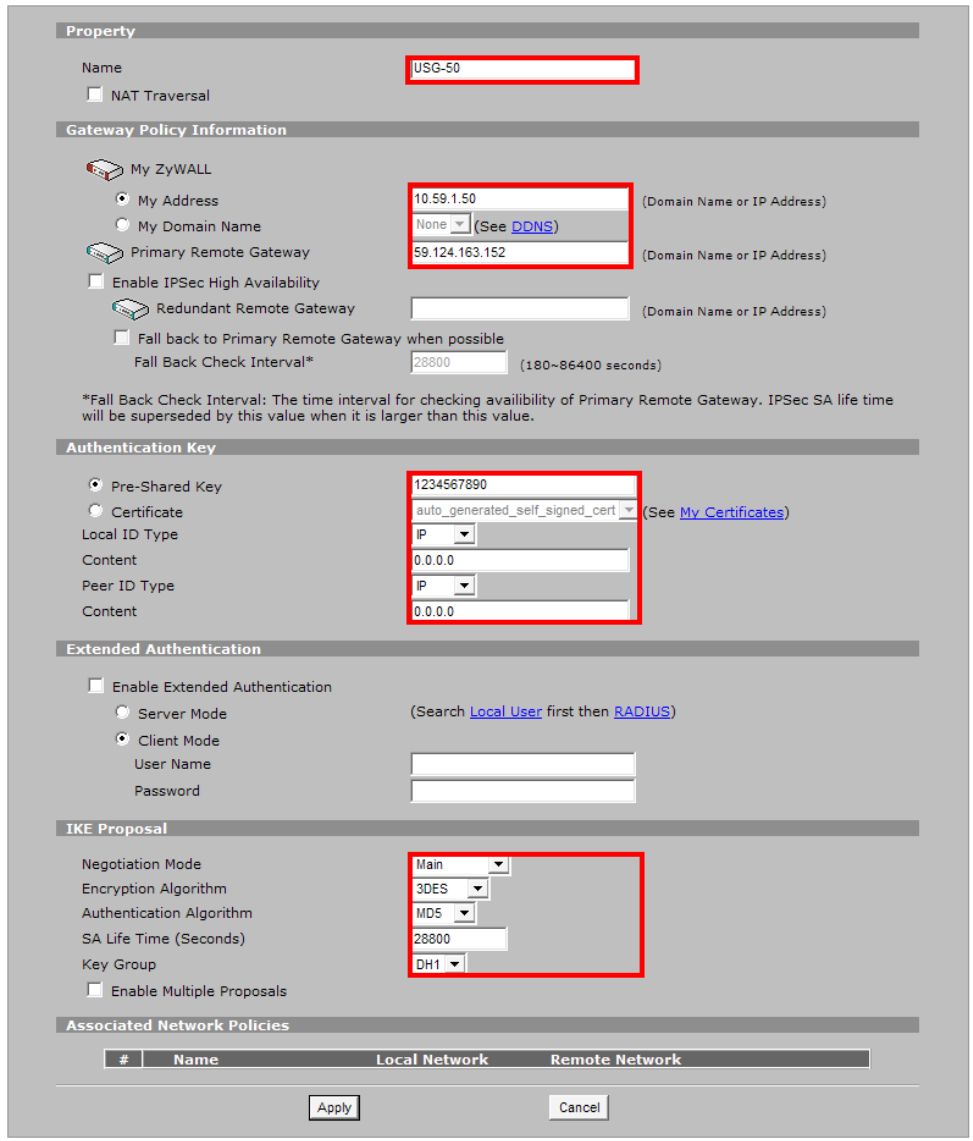


Step 3. To configure the gateway policy, user needs to fill in:

- Policy name
- Gateway information; both local (My ZyWALL) and peer (Remote GW)
- Authentication setting
  - Pre-Shared Key
  - ID Type setting (Local and Peer side)
- Configure the IKE proposal
  - Negotiation mode
  - Encryption algorithm
  - Authentication algorithm
  - Key Group

All contents copyright (c) 2010 ZyXEL Communications Corporation.

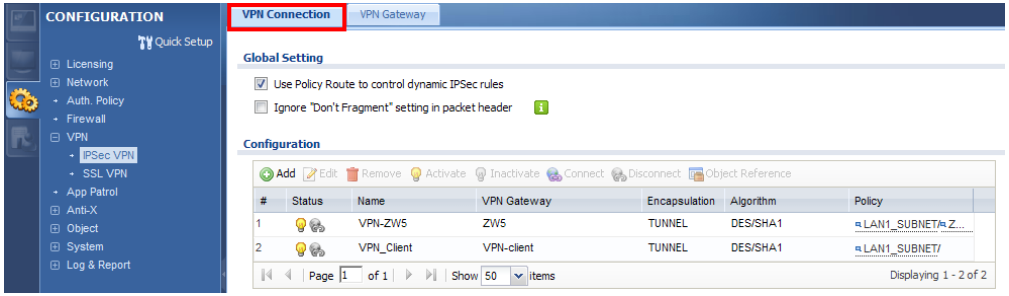




All contents copyright (c) 2010 ZyXEL Communications Corporation.

Step 4. Click **CONFIGURATION > VPN > IPSec VPN > VPN Connection** to open the configuration screen to configure the phase-2 rule.

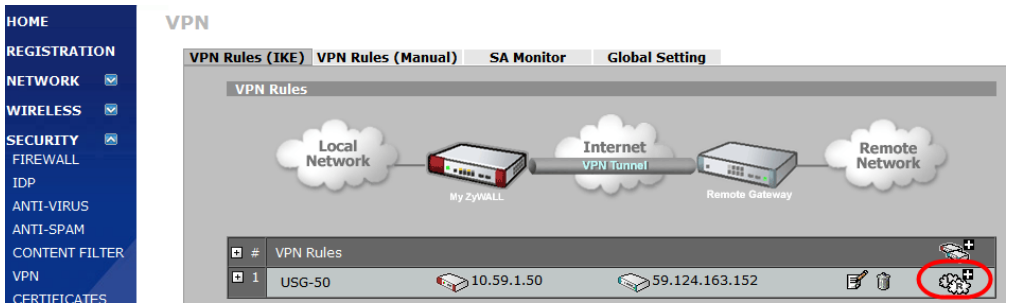
Step 5. Click the **Add** button to add a rule.



Step 6. To configure the phase-2 rule, user needs to fill in:

- VPN connection name
- VPN gateway selection
- Policy for
  - Local network side
  - Remote network side
- Phase-2 settings
  - Active protocol
  - Encapsulation mode
  - Encryption algorithm
  - Authentication algorithm
  - Perfect Forward Secrecy

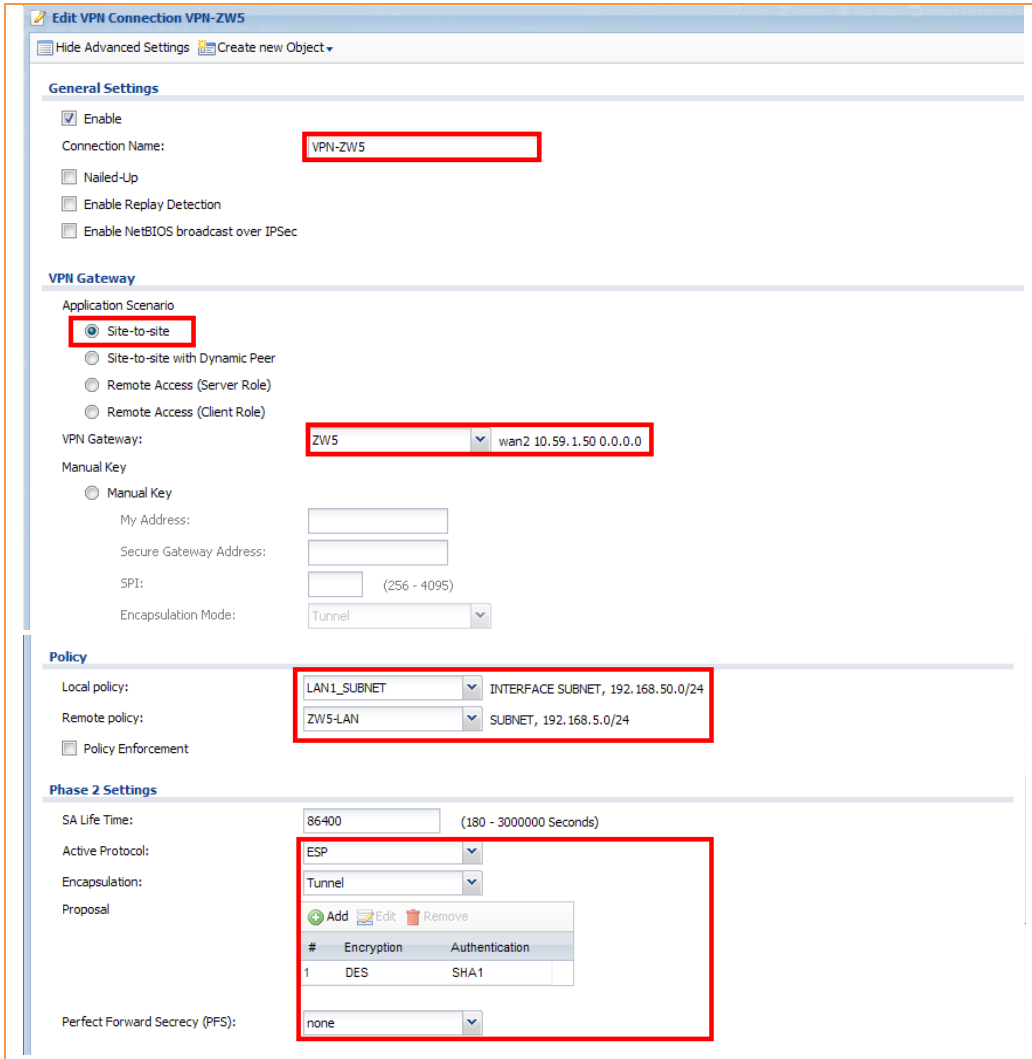
Step 4. Go back to the previous page to see the newly created IKE rule. Click the **Add** button to add a Network policy.

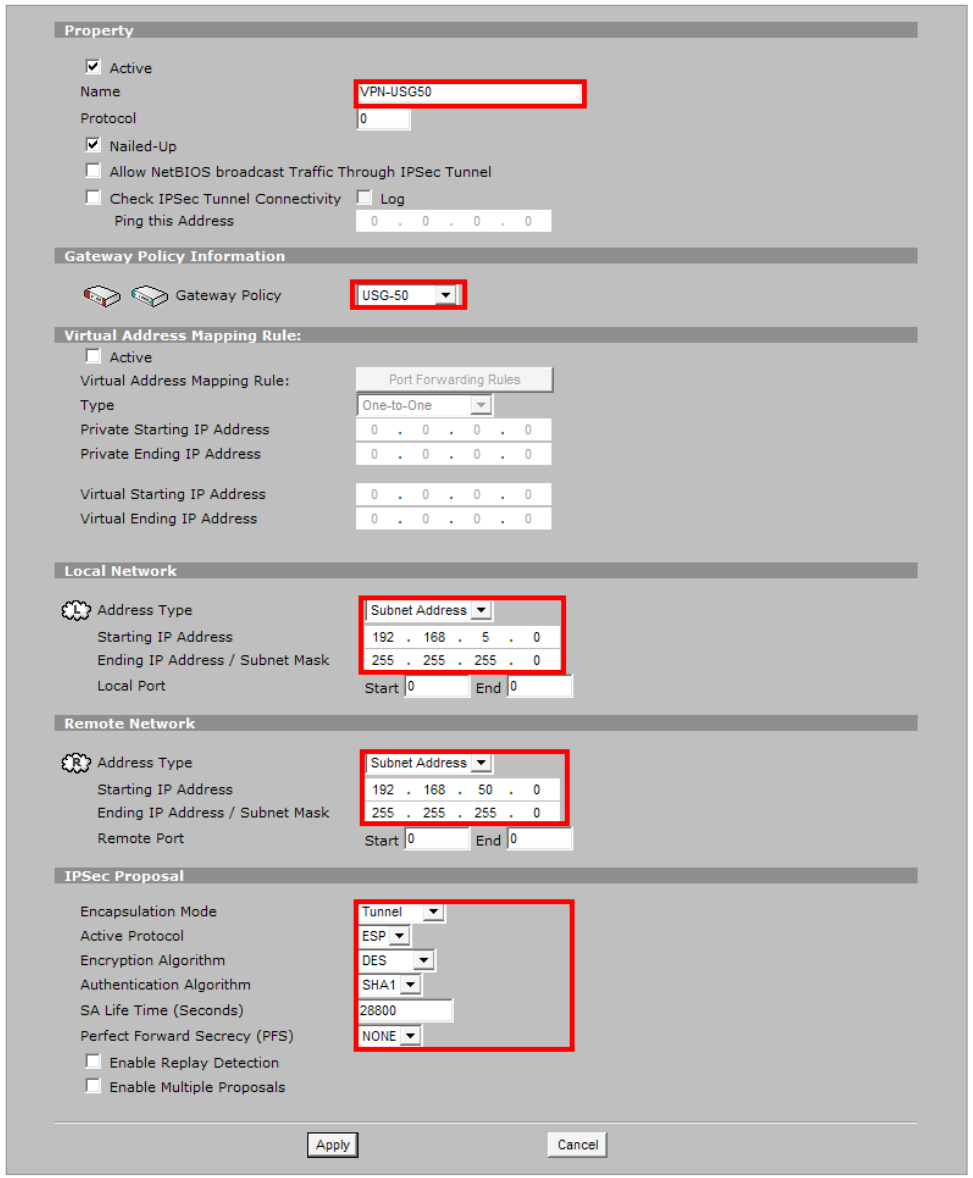


Step 5. To configure the network policy, user needs to fill in:

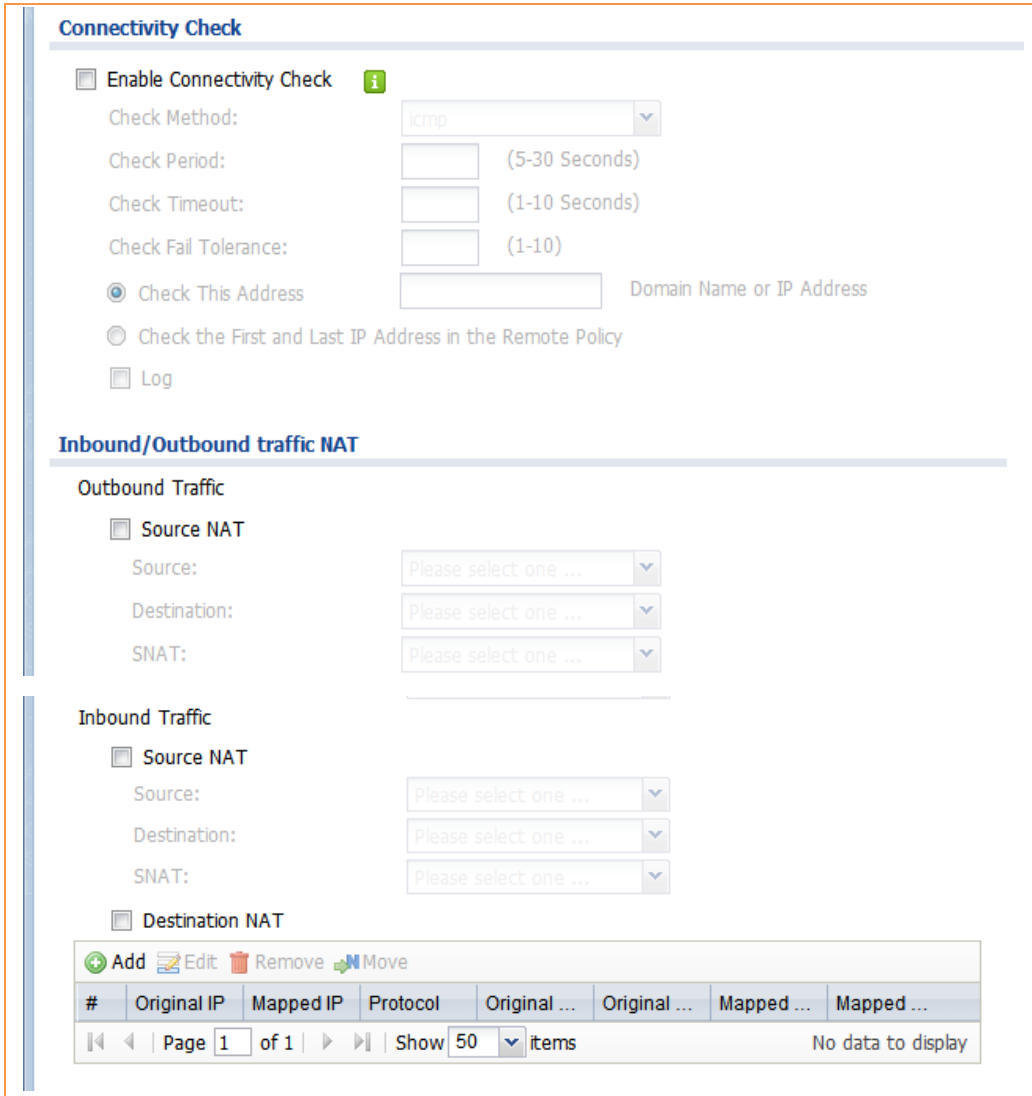
- Policy name
- The gateway rule it is applied to
- Tunnel policy for
  - Local network side
  - Remote network side
- Configure the IPSec proposal
  - Encapsulation mode
  - Active protocol
  - Encryption algorithm
  - Authentication algorithm
  - Perfect Forward Secrecy

All contents copyright (c) 2010 ZyXEL Communications Corporation.

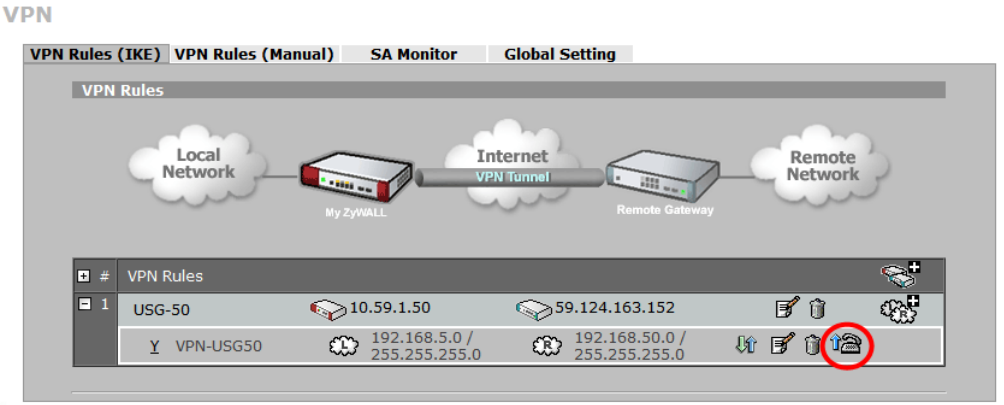




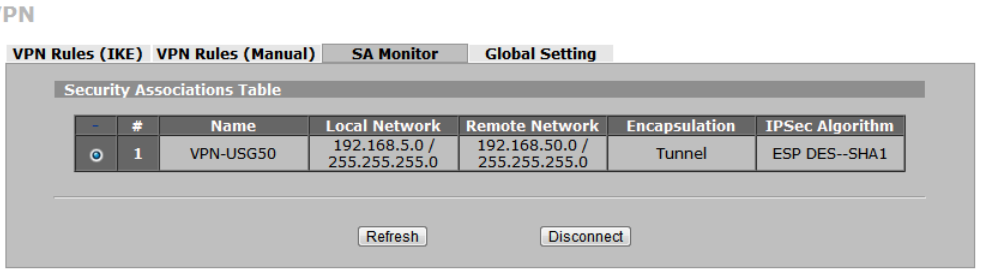
All contents copyright (c) 2010 ZyXEL Communications Corporation.



Step 6. After saving the network policy, user can see the IPSec VPN configuration is complete. Click the **Connect** button to enable the VPN tunnel.

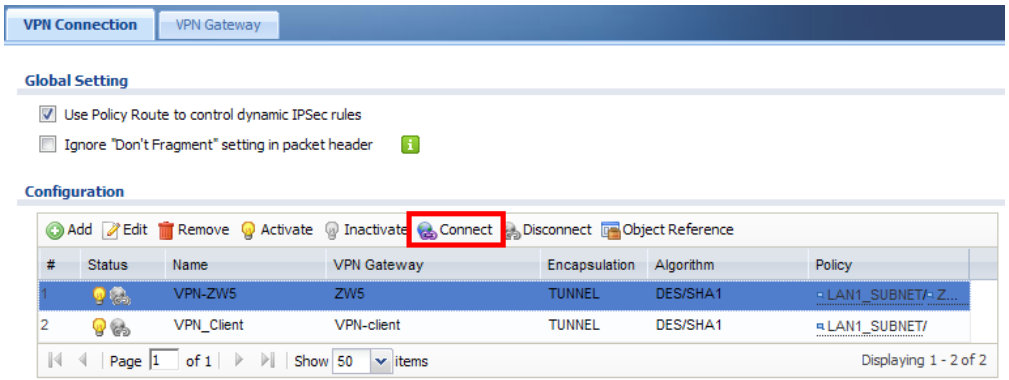


Step 7. After the VPN tunnel is established, user can find the SA information on **SECURITY > VPN > SA Monitor**.

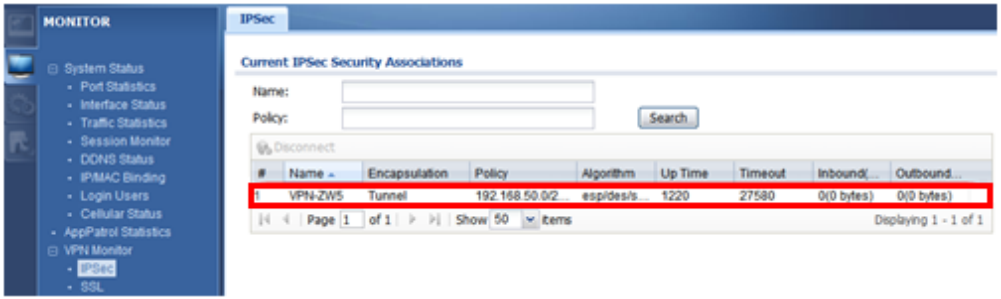


All contents copyright (c) 2010 ZyXEL Communications Corporation.

Step 7. After setting the rule, user can select the rule and click the **Connect** button to establish the VPN link. Once the tunnel is established, a **connected** icon will be displayedin front of the rule.



Step 8. When the VPN tunnel is established, user can find the SA information on **MONITOR > VPN MONITOR > IPSec**.

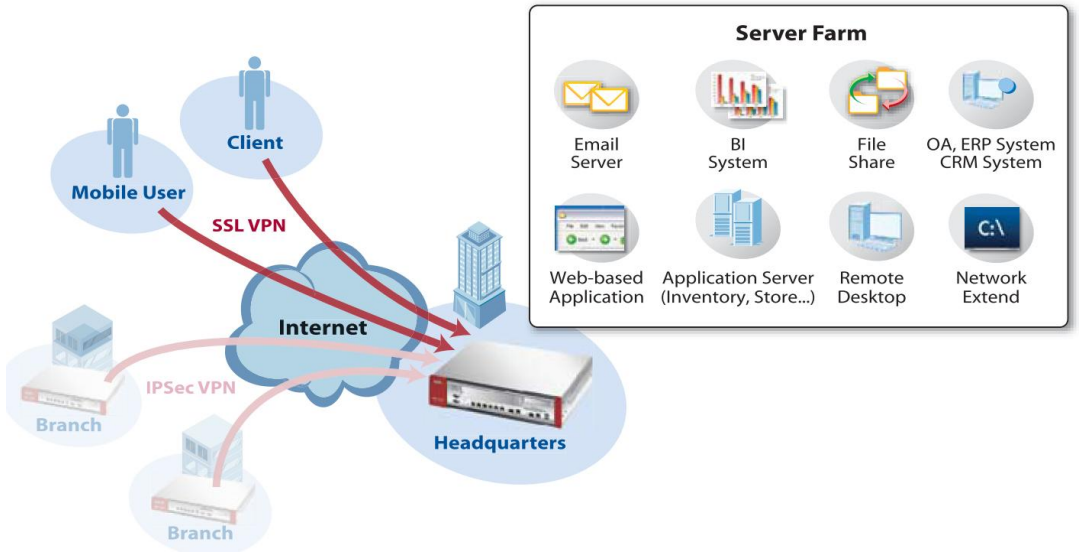


All contents copyright (c) 2010 ZyXEL Communications Corporation.

Scenario 5 — Secure client-to-site connections using IPSec VPN

5.1 Application Scenario

The ZyWALL USG Series can provide secure access between remote locations and corporate resources through the Internet for organizations of any size. Using IPSec VPN, companies can secure connections to branch offices, partners and headquarters.
Road warriors and telecommuters can use SSL or L2TP VPN to safely access the company network without having to install VPN software. ZyWALL USG Series provides a flexible and easy way to enable mobile employees, vendors and partners to confidentially access your network resource for better efficiency.



All contents copyright (c) 2010 ZyXEL Communications Corporation.

5.2 Configuration Guide

Network Conditions:

USG-50:

- WAN IP: 10.59.1.39
- Local subnet: 192.168.50.0/24

ZyWALL-5 UTM:

- WAN IP: 10.59.1.50
- Local subnet: 192.168.5.0/24

IPSec VPN Conditions:

Phase 1:

- Authentication: 1234567890
- Local/Peer ID type: IP 0.0.0.0
- Negotiation: Main mode
- Encryption Algorithm: 3DES
- Authentication Algorithm: MD5
- Key Group: DH1

Phase 2:

- Encapsulation Mode: Tunnel
- Active Protocol: ESP
- Encryption Algorithm: DES
- Authentication Algorithm: SHA1
- Perfect Forward Secrecy: None

Goal to achieve:

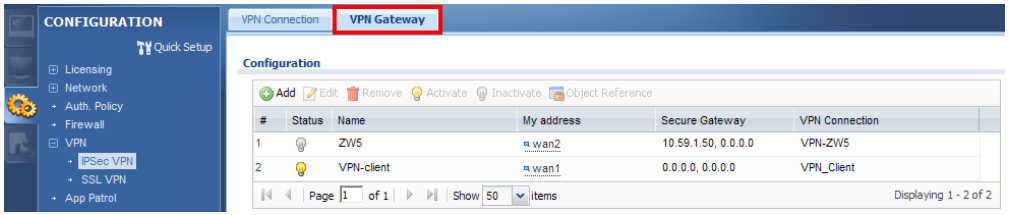
Build up an IPSec VPN tunnel for mobile user's dynamic access to USG-50 or ZyWALL-5 UTM with the above configuration.

All contents copyright (c) 2010 ZyXEL Communications Corporation.

ZLD configuration

Step 1. Click **CONFIGURATION > VPN > IPSec VPN > VPN Gateway** to open the configuration screen.

Step 2. Click the **Add** button to add a VPN gateway rule.



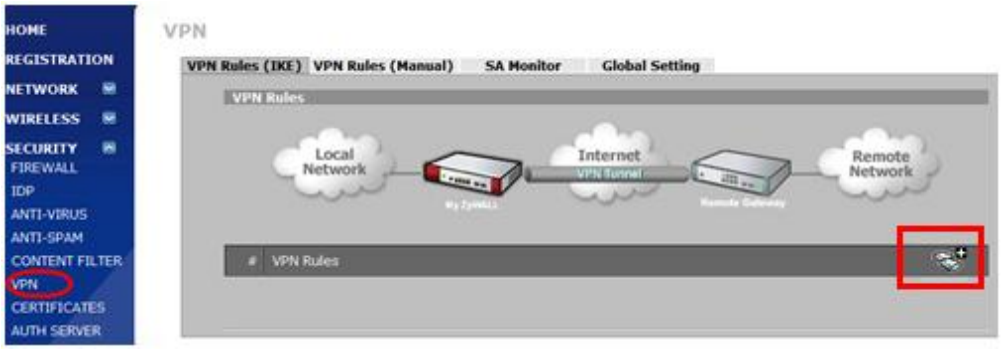
Step 3. To configure the VPN gateway rule, user needs to fill in:

- VPN gateway name
- Gateway address; both local (My Address) and peer (Dynamic Address)
- Authentication setting
  - Pre-Shared Key
  - ID Type setting (Local and Peer side)
- Phase-1 setting
  - Negotiation mode
  - Encryption algorithm
  - Authentication algorithm
  - Key Group

ZyNOS configuration

Step 1. Click **SECURITY > VPN > VPN RULES (IKE)** to open the configuration screen.

Step 2. Click the **Add** button to add a gateway policy.



Step 3. To configure the gateway policy, user needs to fill in:

- Policy name
- Gateway information; both local (My ZyWALL) and peer ("0.0.0.0" for dynamic access)
- Authentication setting
  - Pre-Shared Key
  - ID Type setting (Local and Peer side)
- Configure the IKE proposal
  - Negotiation mode
  - Encryption algorithm
  - Authentication algorithm
  - Key Group

All contents copyright (c) 2010 ZyXEL Communications Corporation.

Edit VPN Gateway VPN-client

Hide Advanced Settings

General Settings

Enable

VPN Gateway Name: VPN-client

Gateway Settings

My Address

Interface: wan1 — DHCP client -- 10.59.1.61/255.255.255.0

Domain Name / IP

Peer Gateway Address

Static Address — Primary: 0.0.0.0 — Secondary: 0.0.0.0

Dynamic Address

Authentication

Pre-Shared Key: 1234567890

Certificate: default (See My Certificates)

Local ID Type: IP

Content: 0.0.0.0

Phase 1 Settings

SA Life Time: 86400 (180 - 3000000 Seconds)

Negotiation Mode: Main

Proposal: Add / Edit / Remove

#	Encryption	Authentication
1	3DES	MD5

Key Group: DH1

NAT Traversal

Dead Peer Detection (DPD)

Extended Authentication

Enable Extended Authentication

Server Mode: default

Client Mode

User Name:

Password:

VPN - GATEWAY POLICY - EDIT

Property

Name: VPN_Client

NAT Traversal

Gateway Policy Information

My ZyWALL

My Address: 10.59.1.50 (Domain Name or IP Address)

My Domain Name: None (See DDNS)

Primary Remote Gateway: 0.0.0.0 (Domain Name or IP Address)

Enable IPSec High Availability

Redundant Remote Gateway: (Domain Name or IP Address)

Fall back to Primary Remote Gateway when possible

Fall Back Check Interval*: 28800 (180~86400 seconds)

*Fall Back Check Interval: The time interval for checking availibility of Primary Remote Gateway. IPSec SA life time will be superseded by this value when it is larger than this value.

Authentication Key

Pre-Shared Key: 1234567890

Certificate: auto_generated_self_signed_cert (See My Certificates)

Local ID Type: IP

Content: 0.0.0.0

Peer ID Type: IP

Content: 0.0.0.0

Extended Authentication

Enable Extended Authentication

Server Mode (Search Local User first then RADIUS)

Client Mode

User Name

Password

IKE Proposal

Negotiation Mode: Main

Encryption Algorithm: 3DES

Authentication Algorithm: MD5

SA Life Time (Seconds): 28800

Key Group: DH1

Enable Multiple Proposals

Associated Network Policies

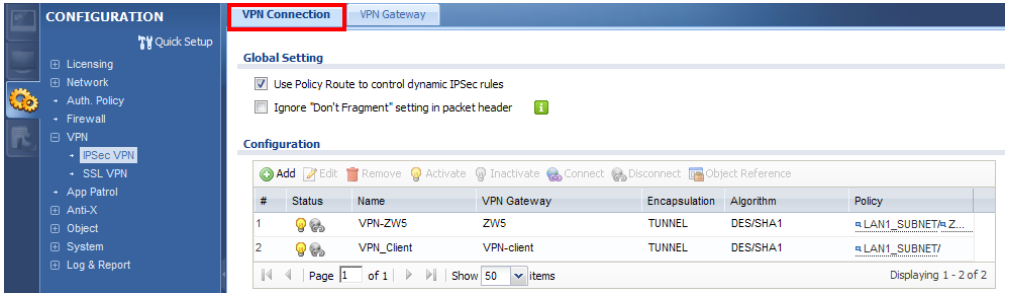
#	Name	Local Network	Remote Network

Apply Cancel

All contents copyright (c) 2010 ZyXEL Communications Corporation.

Step 4. Click **CONFIGURATION > VPN > IPSec VPN > VPN Connection** to open the configuration screen to configure the phase-2 rule.

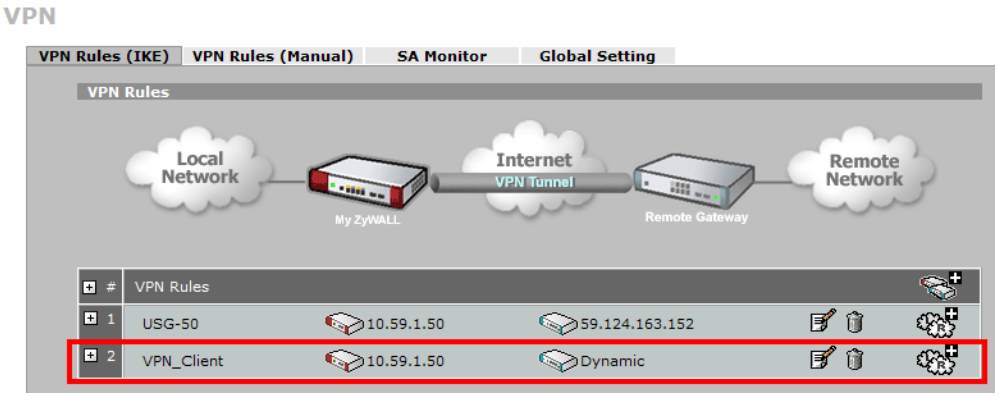
Step 5. Click **Add** button to add a rule.



Step 6. To configure the phase-2 rule, user needs to fill in:

- VPN connection name
- VPN gateway selection
- Policy for
  - Local network side
  - Remote network side
- Phase-2 setting
  - Active protocol
  - Encapsulation mode
  - Encryption algorithm
  - Authentication algorithm
  - Perfect Forward Secrecy

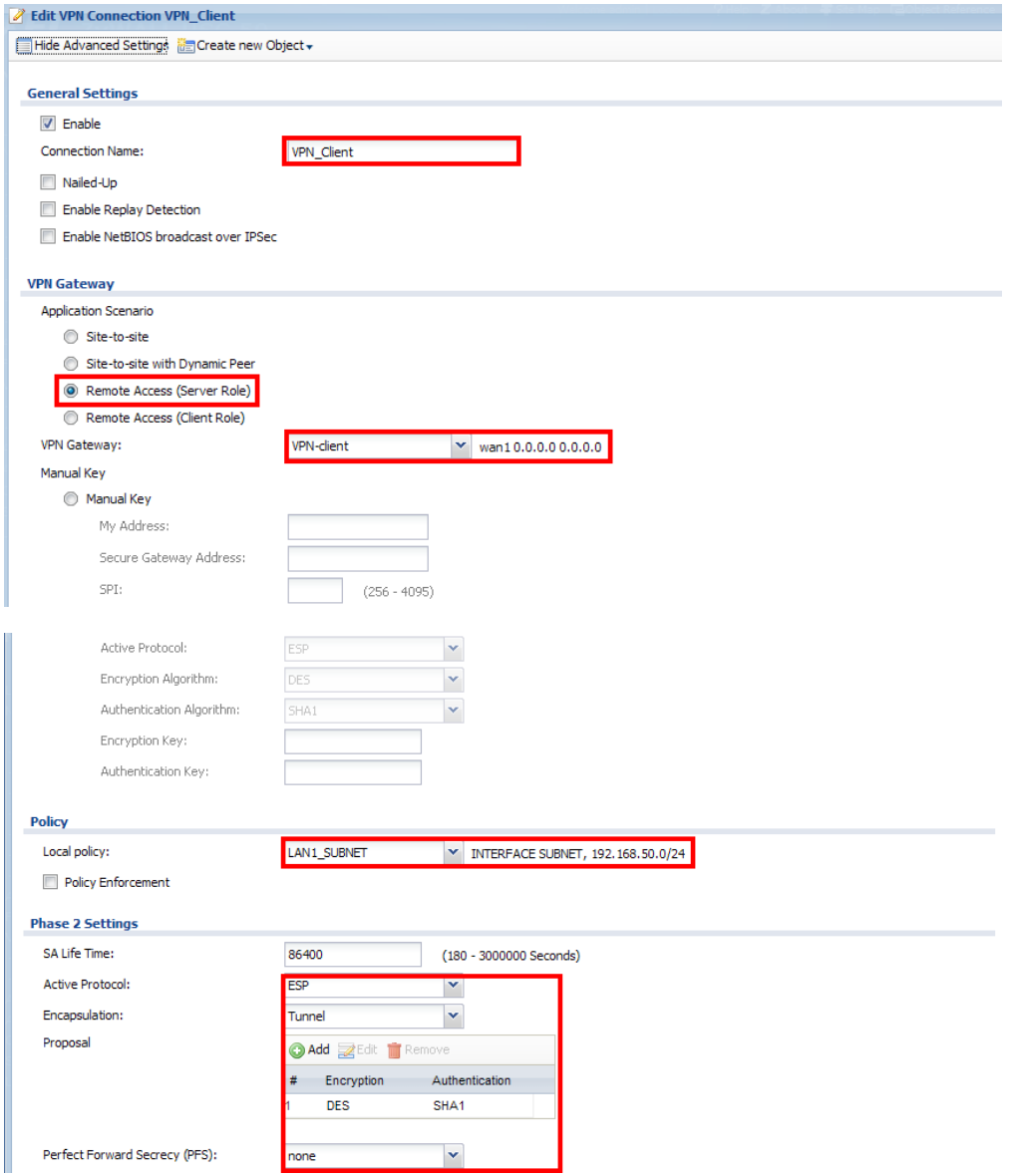
Step 4. Go back to the previous page, to see the newly created IKE rule with the destination **Dynamic**. Click the **Add** button to add a Network policy.

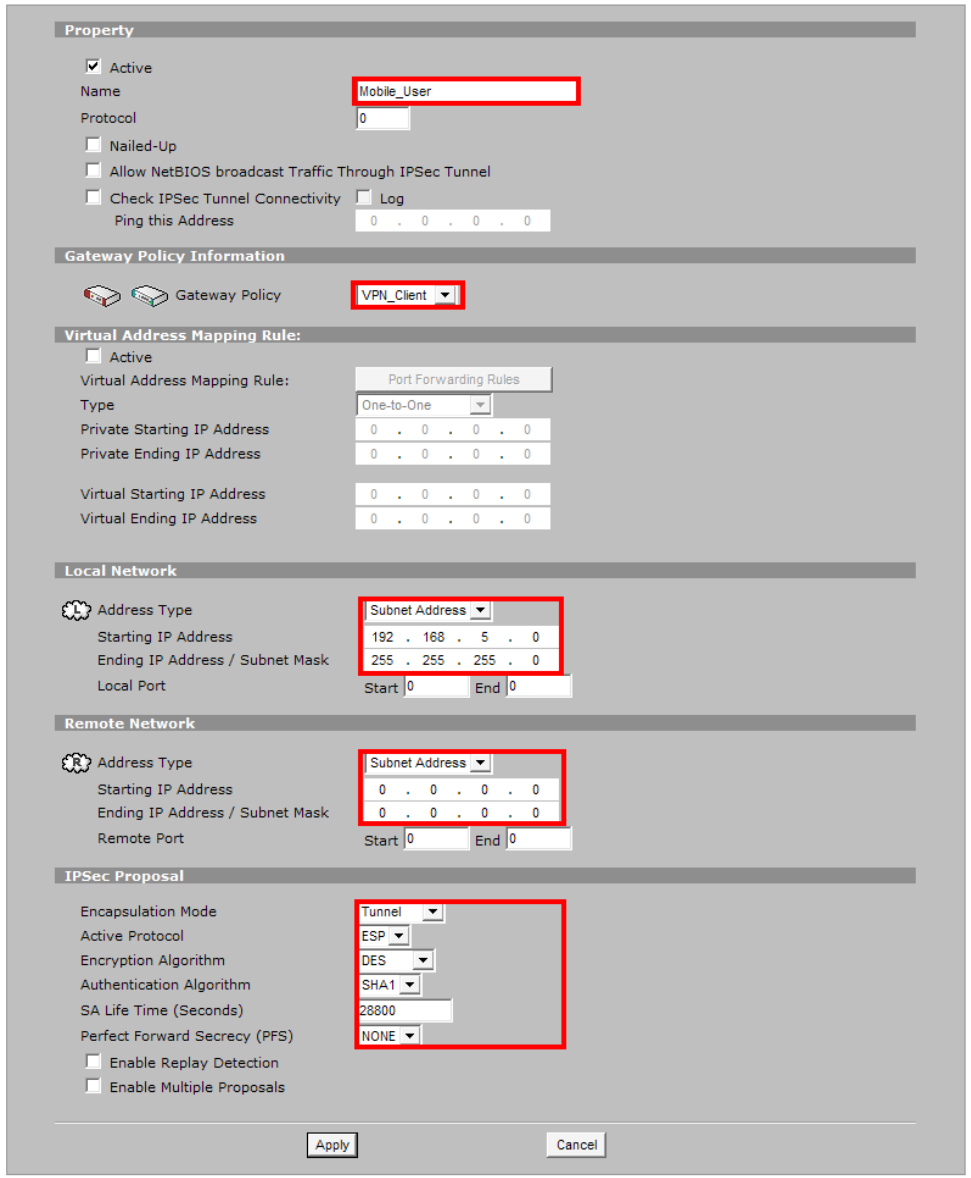


Step 5. To configure the network policy, user needs to fill in:

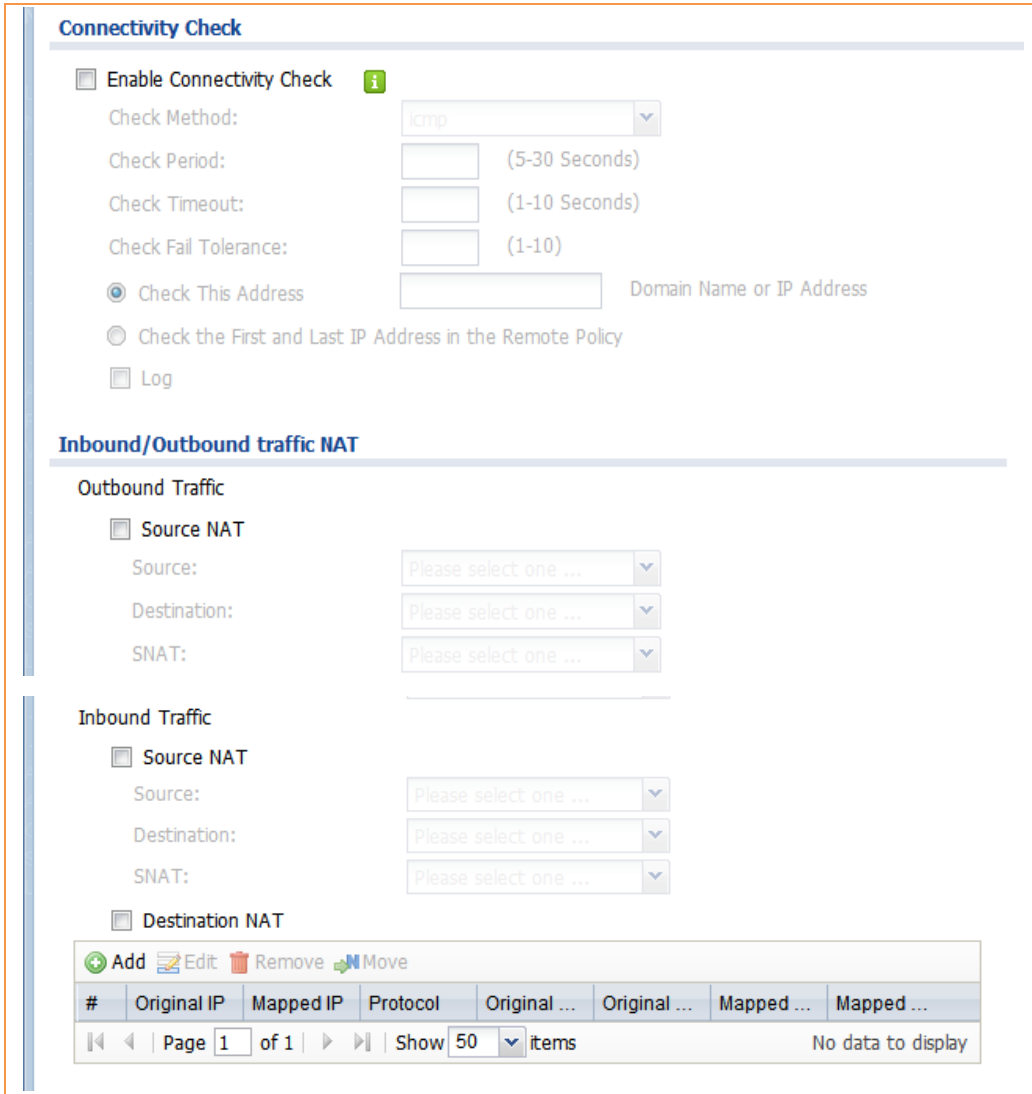
- Policy name
- The gateway rule it is applied to
- Tunnel policy for
  - Local network side
  - Remote network side; “0.0.0.0” means for dynamic access
- Configure the IPSec proposal
  - Encapsulation mode
  - Active protocol
  - Encryption algorithm
  - Authentication algorithm
  - Perfect Forward Secrecy

All contents copyright (c) 2010 ZyXEL Communications Corporation.

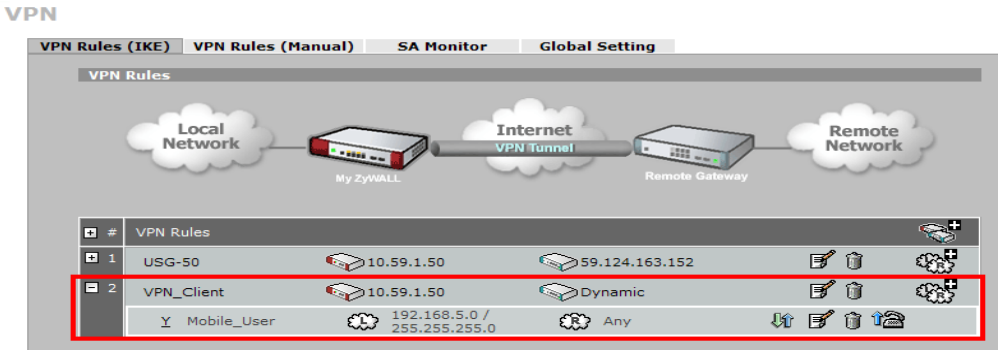




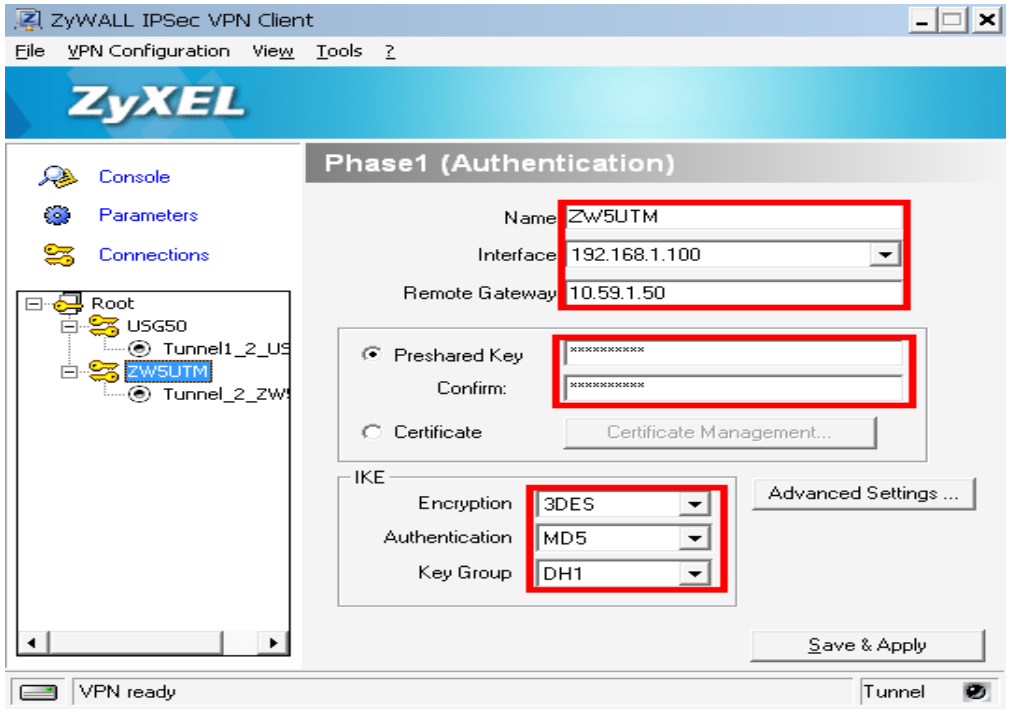
All contents copyright (c) 2010 ZyXEL Communications Corporation.



Step 6. After setting up the network policy, user can see the IPSec VPN configuration is complete. Note that the destination is **Any**.

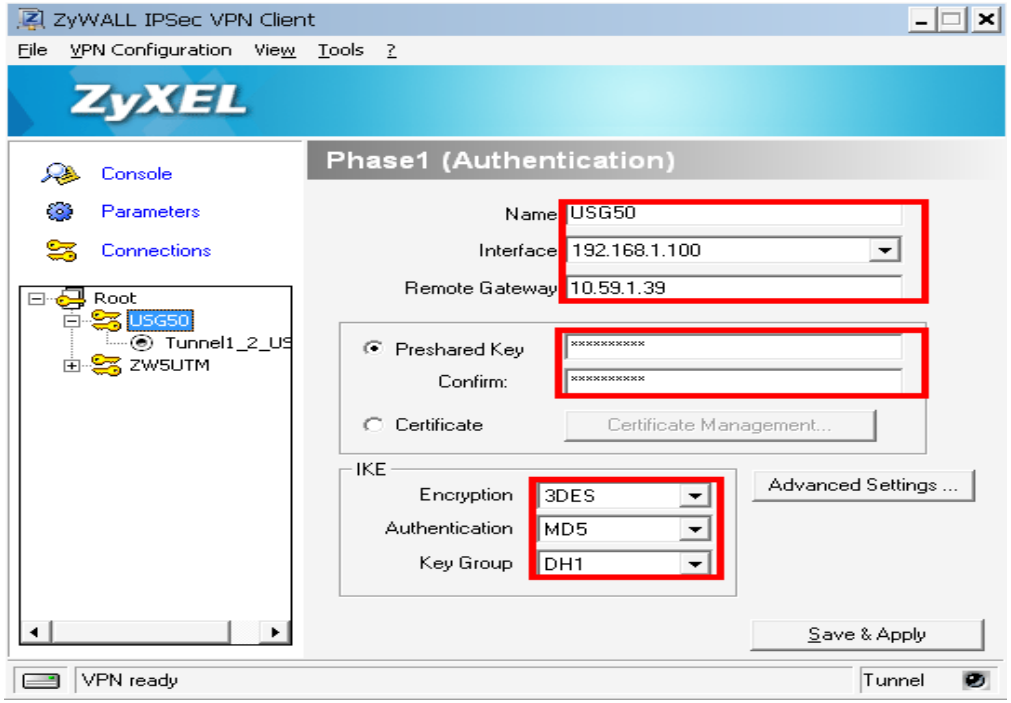


Step 7. Start the ZyXEL IPSec VPN Client. Fill in the Phase-1 configuration.

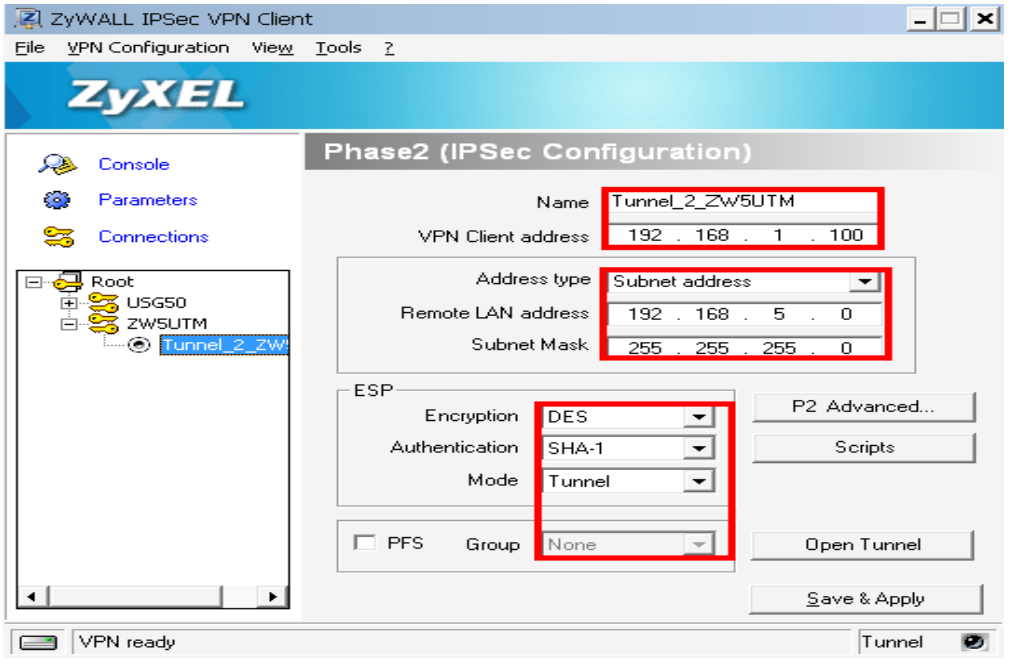


All contents copyright (c) 2010 ZyXEL Communications Corporation.

Step 7. Start the ZyXEL IPSec VPN Client. Fill in the Phase-1 configuration. Note that the USG series does not support the “Config Mode” in phase-1 advanced setting, thus users must avoid selecting it when performing configuration.

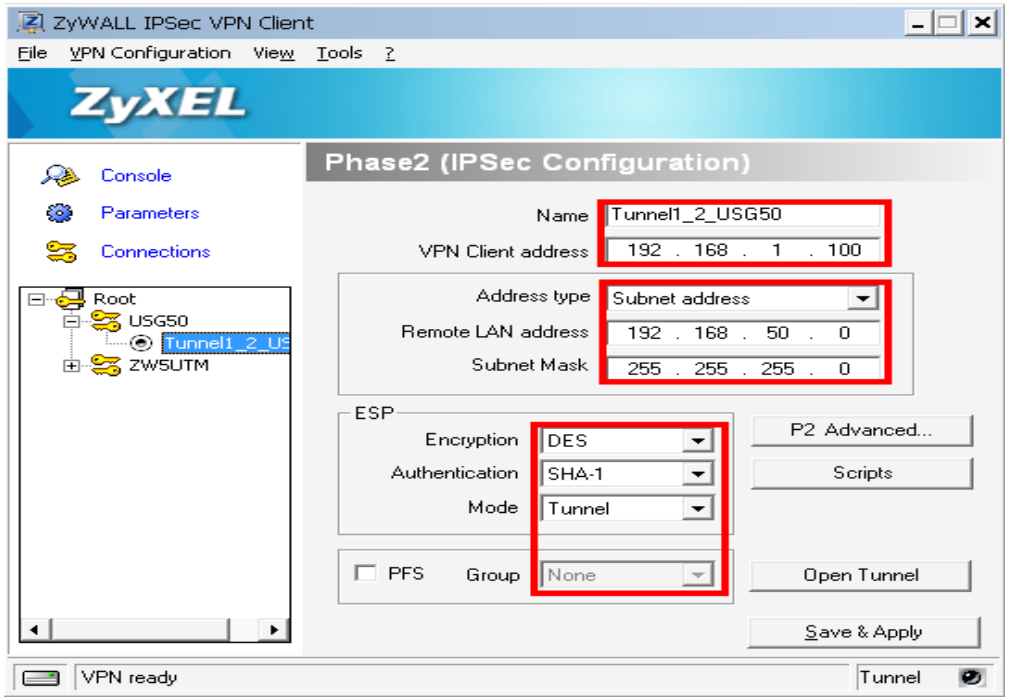


Step 8. Configure the phase-2 parameters.

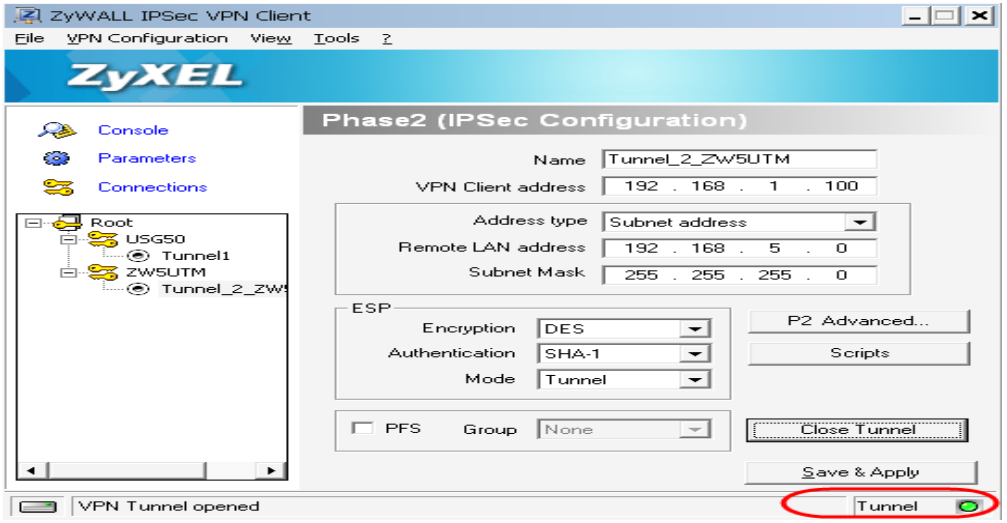


All contents copyright (c) 2010 ZyXEL Communications Corporation.

Step 8. Configure the phase-2 parameters.

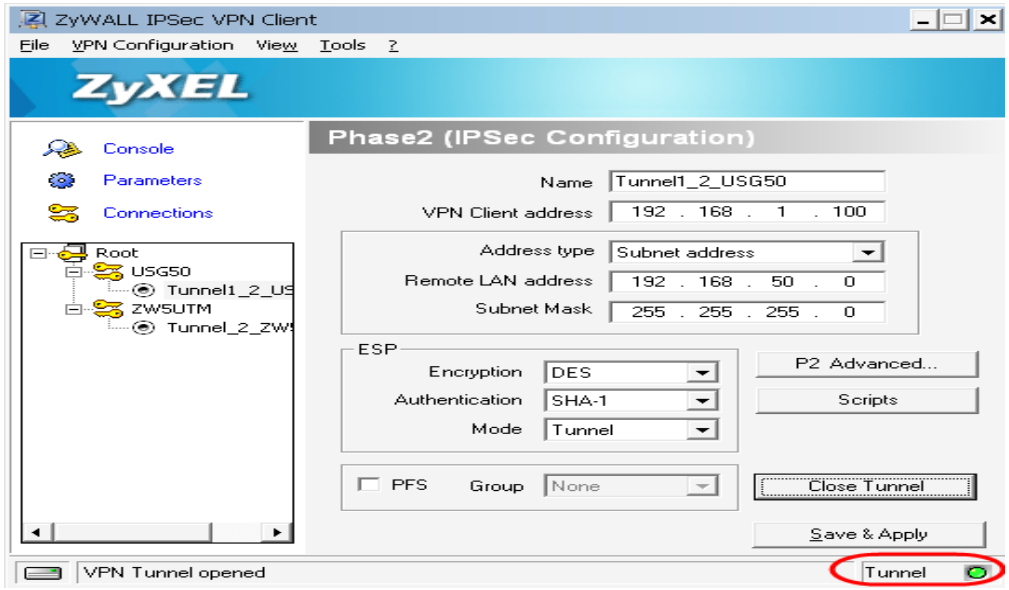


Step 9. Because it is a dynamic rule, user MUST enable it from the VPN client. Click **Open Tunnel** to enable it. The icon will change to green if established successfully.

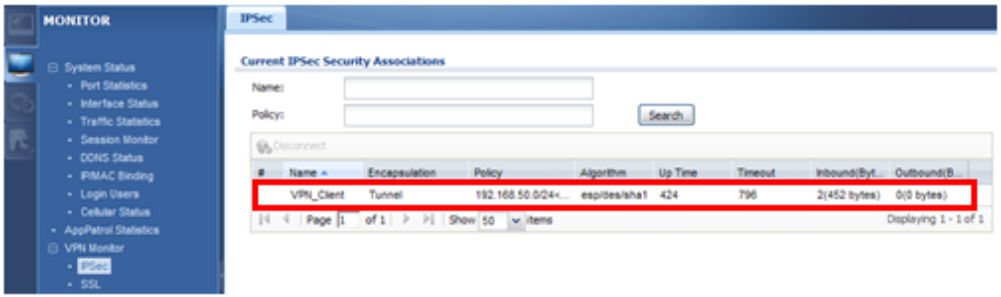


All contents copyright (c) 2010 ZyXEL Communications Corporation.

Step 9. Because it is a dynamic rule, user MUST enable it from the VPN client. Click **Open Tunnel** to enable it. The icon will change to green if established successfully.



Step 10. When the VPN tunnel is established, user can find the SA information on **MONITOR > VPN MONITOR > IPSec**.



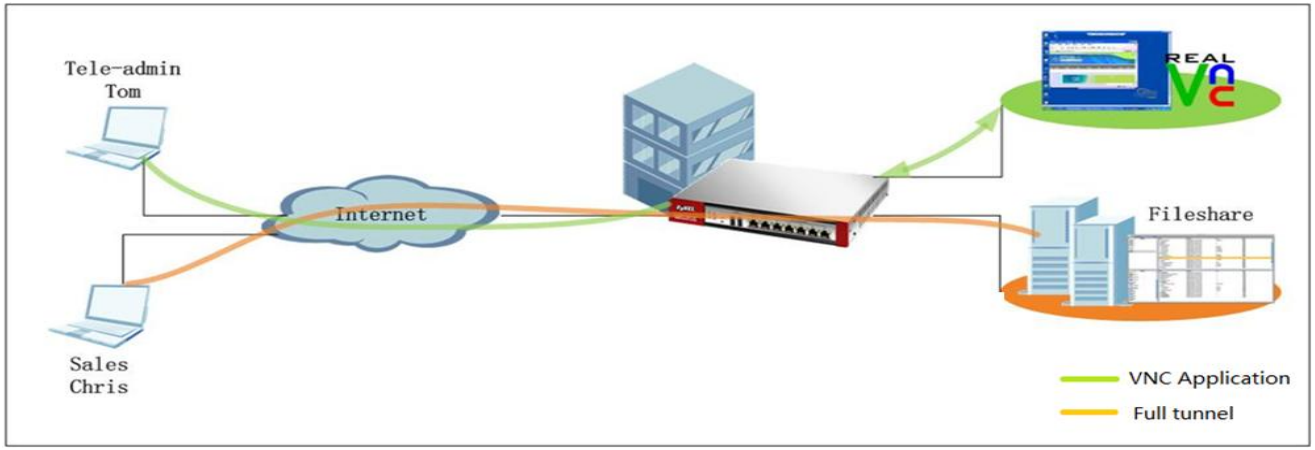
All contents copyright (c) 2010 ZyXEL Communications Corporation.

Scenario 6 — Deploying SSL VPN for Tele-workers to Access Company Resources

6.1 Application Scenario

Tele-workers who work out of the office sometimes need to access company resources by a secured way. While building an IPSec tunnel to the company gateway is an option, the Windows VPN client configuration is too complicated, and for an easier way to configure IPSec VPN, it requires installation of additional IPSec VPN client software. The USG ZyWALL provides an SSL VPN function, which enables teleworkers to access company resources through a secured VPN tunnel with little effort. All they need on their PC is a browser. Besides, in SSL VPN, the network administrator can define different access rules to allow different users to access different company resources.

For example, the network administrator can set up an SSL VPN rule to allow administrator Tom remotely control company servers by RDP or VNC through SSL VPN tunnel. He can also set up an SSL VPN Full tunnel rule to allow sales Chris to remotely access company file-share resources to conduct his important daily job.



NOTE: USG 50 supports RDP, VNC, WEB link application and SSL VPN full tunnel, but doesn't support SSL VPN file-share and OWA applications so far. If the remote clients want to use file-share and OWA through SSL VPN, they can use SSL VPN full tunnel mode (Security Extender) as a workaround.

All contents copyright (c) 2010 ZyXEL Communications Corporation.

6.2 Configuration Guide

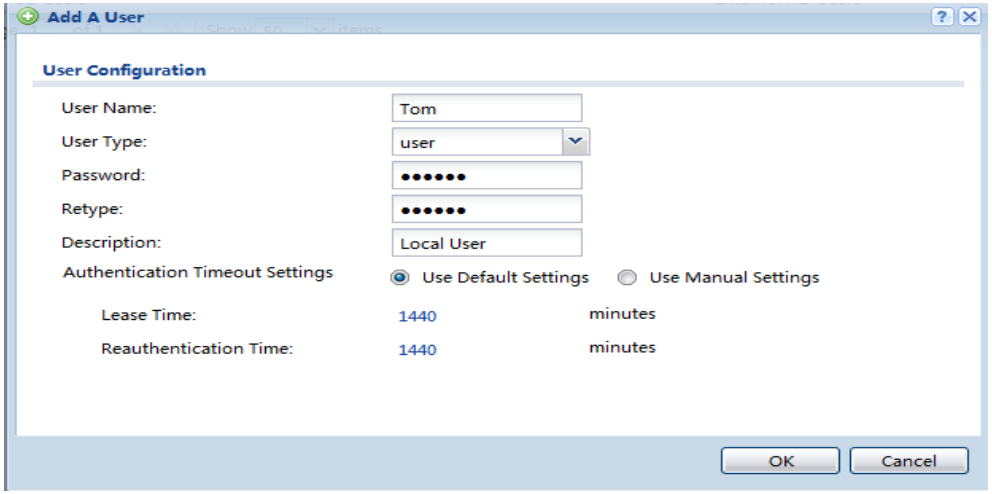
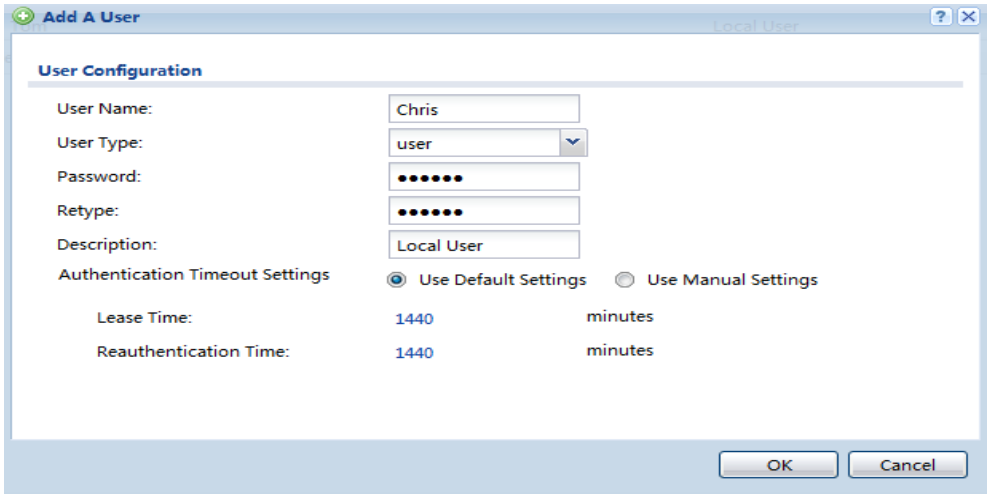
Network Conditions:

- WAN IP: 172.25.27.62
- LAN subnet: 192.168.1.0/24
- VNC server IP: 192.168.1.5

Goals to achieve:

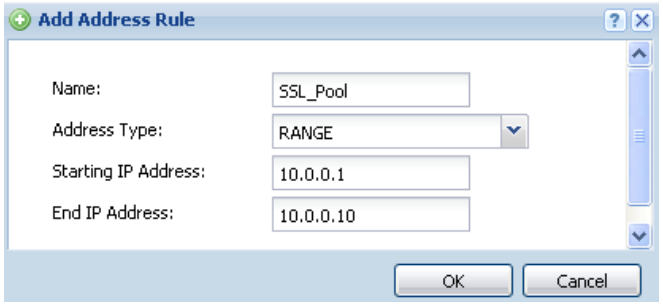
1) Tom in tele-admin group can VNC to the internal server 192.168.1.5 by SSL VPN application.
2) Chris in sales group can access company fileshare resources in the LAN subnet through SSL VPN full tunnel.

All contents copyright (c) 2010 ZyXEL Communications Corporation.

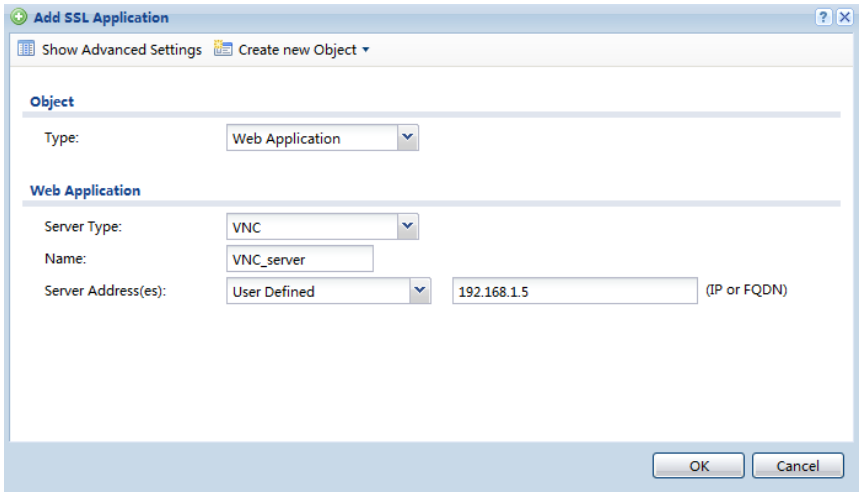
ZLD configuration	ZyNOS configuration
Step 1. Create two local user accounts for Tom and Chris on USG50. Go to **Configuration > Object > User/Group**, add two local user accounts for Tom and Chris:   	ZyNOS ZyWALL does not support SSL VPN.

All contents copyright (c) 2010 ZyXEL Communications Corporation.

Step 2. Go to **Configuration > Object > Address**. Add an IP address pool for the SSL VPN full tunnel mode access (Security Extender).



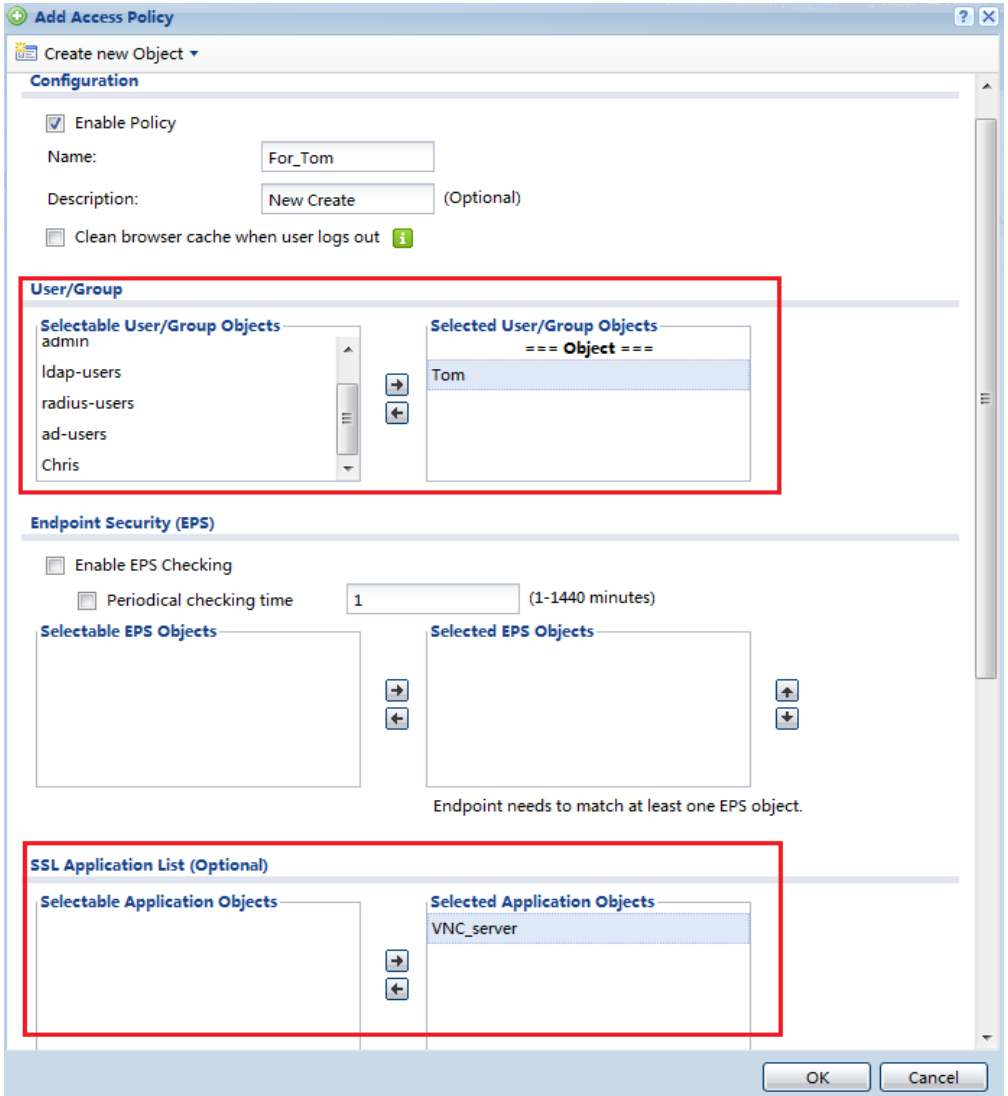
Step3. Go to **Configuration > Object > SSL Application**. Create an SSL application object for the VNC server.



All contents copyright (c) 2010 ZyXEL Communications Corporation.

Step4. Go to **Configuration > VPN > SSL VPN**. Add an SSL VPN rule for Tom to access.

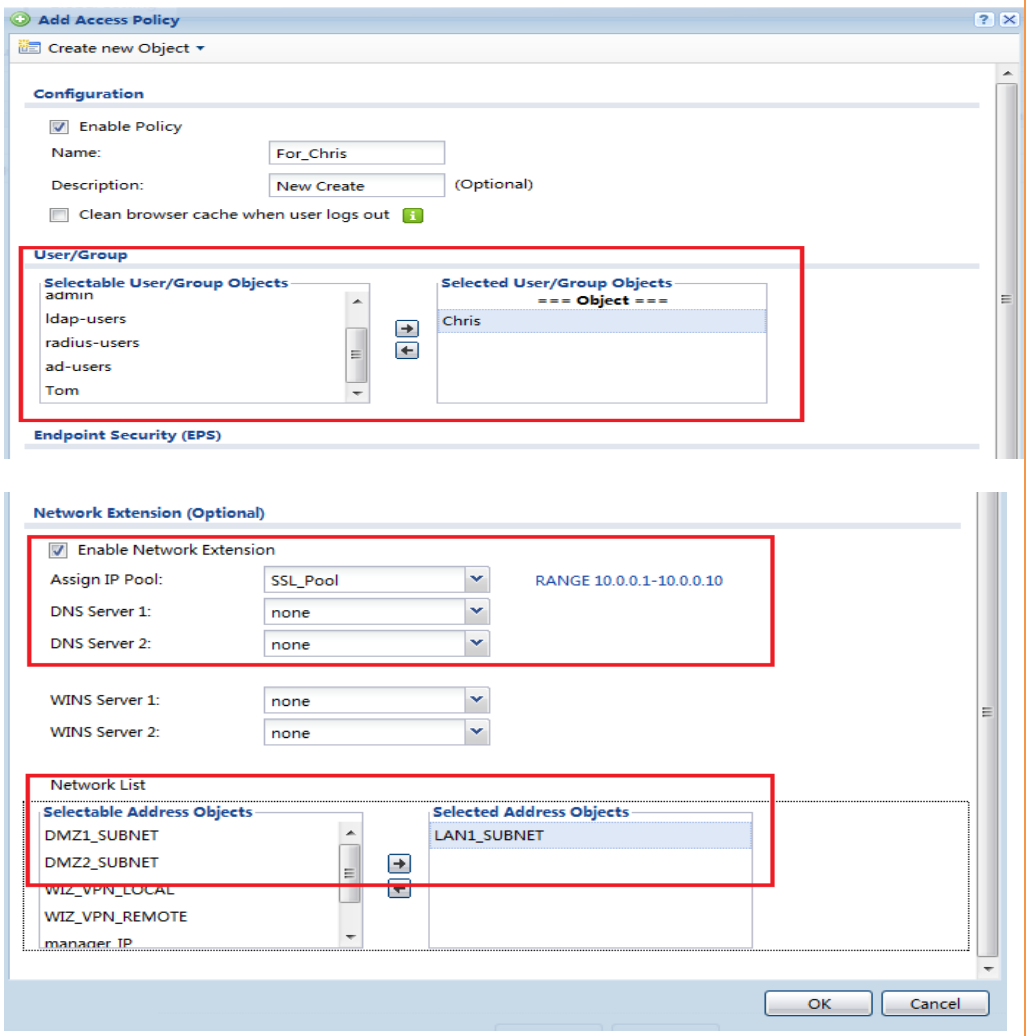
- Allow the user “Tom” to access this rule.
- Add the VNC application to SSL Application.



All contents copyright (c) 2010 ZyXEL Communications Corporation.

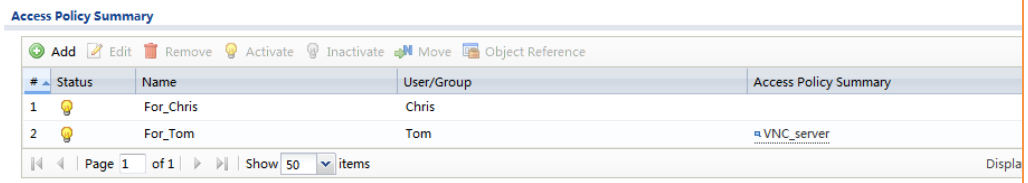
Step5. Go to **Configuration > VPN > SSL VPN**. Add an SSL VPN rule for Chris to access.

- Allow the user “Chris” to access this rule.
- Enable Network Extension, assign the address pool for SSL VPN clients, and select the USG internal network to allow SSL VPN clients to access.



All contents copyright (c) 2010 ZyXEL Communications Corporation.

Check the created policies as below:



Scenario Verification

a. Log in with user “Tom”:

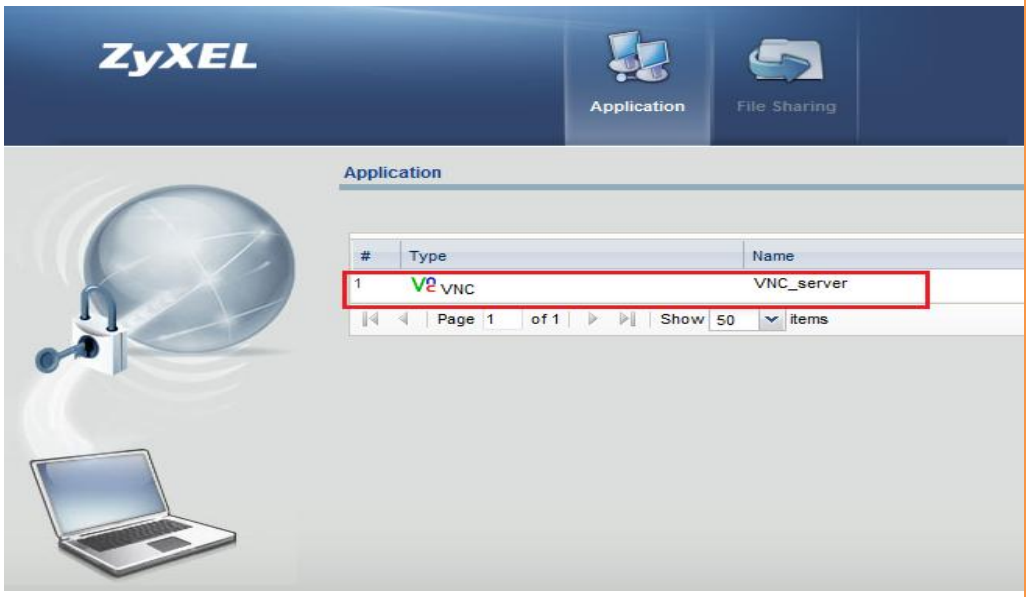
Open the USG login page. Make sure Java is installed and enabled in your browser. Use user “Tom” to log into SSL VPN.

NOTE: To use the SSL VPN RDP application, user must use IE.

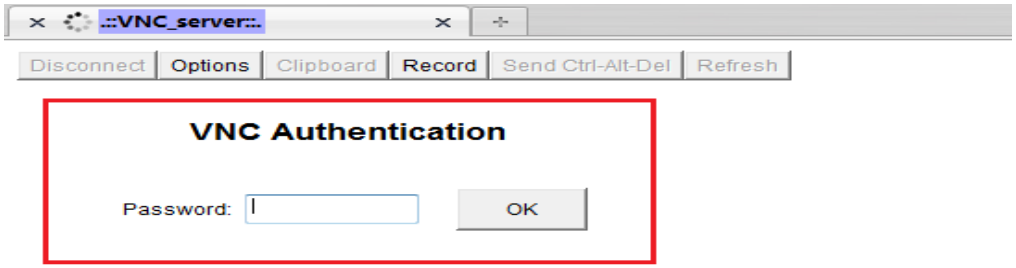
ZyXEL
ZyWALL USG 1000
Enter User Name/Password and click to login.
User Name: Tom
Password:
One-Time Password: (Optional)
(max. 63 alphanumeric, printable characters and no spaces)
Login
SSL VPN
Note:
1. Turn on Javascript and Cookie setting in your web browser.
2. Turn off Popup Window Blocking in your web browser.
3. Turn on Java Runtime Environment (JRE) in your web browser.

All contents copyright (c) 2010 ZyXEL Communications Corporation.

SSL VPN is established. You can see the VNC server on the VPN portal.



User can just click on the VNC application and access the VNC server.



Input the correct password for VNC login, and click OK, the VNC connection will be established.

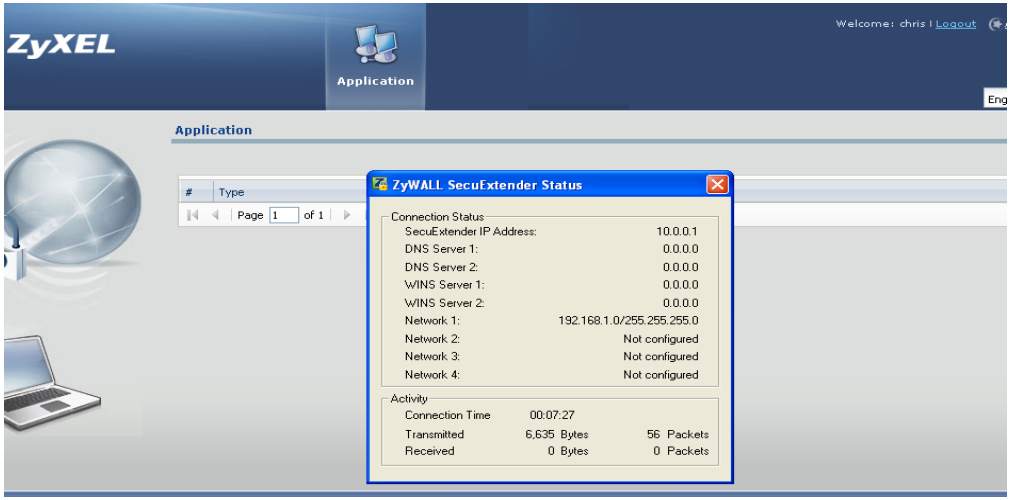
All contents copyright (c) 2010 ZyXEL Communications Corporation.

b. Log in with user “Chris”:

Open the USG login page. Make sure Java is installed and enabled in your browser. Use user “Chris” to log into SSL VPN.

ZyXEL
ZyWALL USG 1000
Enter User Name/Password and click to login.
User Name:
Chris
Password:
One-Time Password:
(Optional)
(max. 63 alphanumeric, printable characters and no spaces)
Login
SSL VPN
Note:
1. Turn on Javascript and Cookie setting in your web browser.
2. Turn off Popup Window Blocking in your web browser.
3. Turn on Java Runtime Environment (JRE) in your web browser.

Full tunnel SSL VPN (Security Extender) will be established.

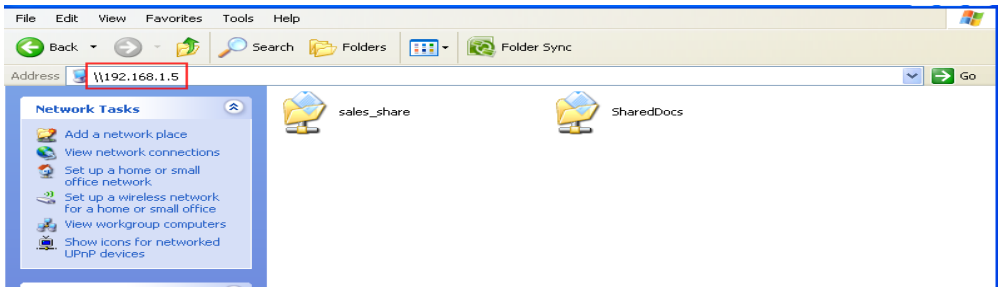


All contents copyright (c) 2010 ZyXEL Communications Corporation.

You can check the client's routing table after the full tunnel is established.

```
C:\Documents and Settings\Administrator>route print
===========================================================================
Interface List
0x1 ........................... MS TCP Loopback interface
0x2 ...00 1b 78 86 b6 89 ...... Realtek RTL8169/8110 Family Gigabit Ethernet NI
 - Packet Scheduler Miniport
0x40004 ...00 53 45 00 00 00 ...... WAN (PPP/SLIP) Interface
===========================================================================
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0    172.25.27.252    172.25.27.35       2
          0.0.0.0          0.0.0.0    172.25.27.254    172.25.27.35      20
         10.0.0.1  255.255.255.255        127.0.0.1       127.0.0.1      50
   10.255.255.255  255.255.255.255         10.0.0.1        10.0.0.1      50
        127.0.0.0        255.0.0.0        127.0.0.1       127.0.0.1       1
      172.20.0.0      255.255.0.0    172.25.27.254    172.25.27.35       2
      172.23.0.0      255.255.0.0    172.25.27.254    172.25.27.35       2
      172.25.0.0      255.255.0.0    172.25.27.254    172.25.27.35       2
      172.25.5.0    255.255.255.0    172.25.27.254    172.25.27.35       2
     172.25.27.0    255.255.255.0     172.25.27.35    172.25.27.35      20
    172.25.27.35  255.255.255.255        127.0.0.1       127.0.0.1      20
  172.25.255.255  255.255.255.255     172.25.27.35    172.25.27.35      20
     192.168.1.0    255.255.255.0    192.168.200.1        10.0.0.1       1
   192.168.200.1  255.255.255.255         10.0.0.1        10.0.0.1       1
       224.0.0.0        240.0.0.0         10.0.0.1        10.0.0.1      50
       224.0.0.0        240.0.0.0     172.25.27.35    172.25.27.35      20
  255.255.255.255  255.255.255.255         10.0.0.1        10.0.0.1       1
```

The client can access the LAN resources by their private IP's as if he were in the same local network with the LAN hosts. In this example, the user can access the file share server in USG LAN subnet.


File Edit View Favorites Tools Help
Back Search Folders Folder Sync
Address \\192.168.1.5
Go
Network Tasks
Add a network place
View network connections
Set up a home or small office network
Set up a wireless network for a home or small office
View workgroup computers
Show icons for networked UPnP devices
sales_share
SharedDocs

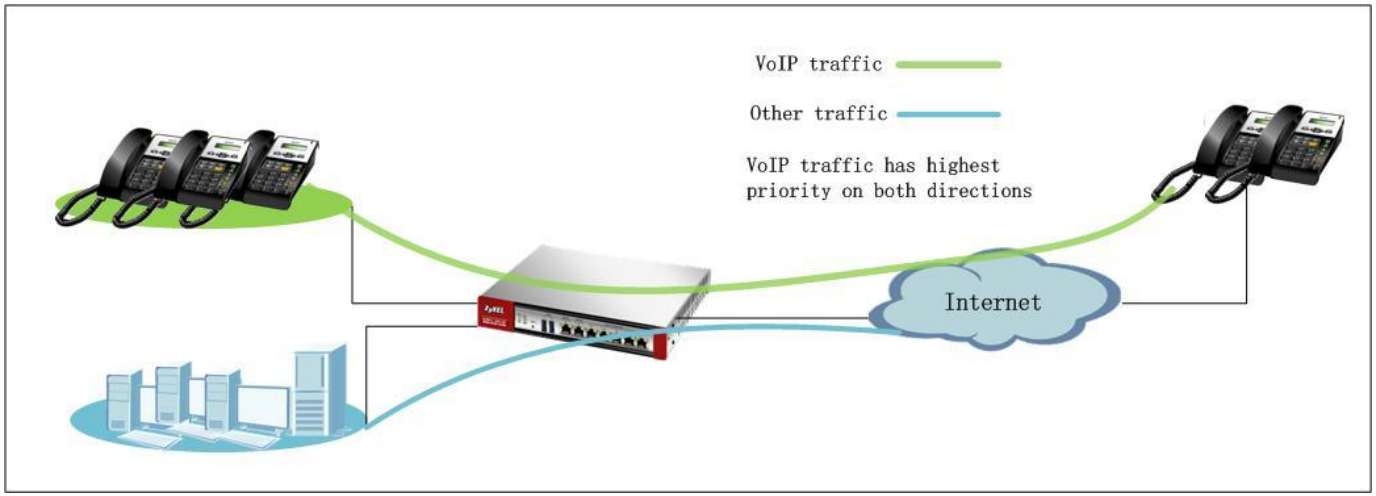
All contents copyright (c) 2010 ZyXEL Communications Corporation.

Scenario 7 — Reserving Highest Bandwidth Management Priority for VoIP Traffic

7.1 Application Scenario

In an enterprise network, there are various types of traffic. But the company Internet connection bandwidth is limited to a specific value. All this traffic will contend to use the limited bandwidth, which may result in some important traffic, for example, VoIP traffic getting slow or even starved. Therefore, intelligent bandwidth management for improved productivity becomes a matter of high concern for network administrators. ZyXEL ZyWALL provides Bandwidth Management (BWM) function to effectively manage bandwidth according to different flexible criteria.

VoIP traffic is quite sensitive to delay and jitter. Therefore, in an enterprise company, VoIP traffic should usually be awarded the highest priority over all other types of traffic.



All contents copyright (c) 2010 ZyXEL Communications Corporation.

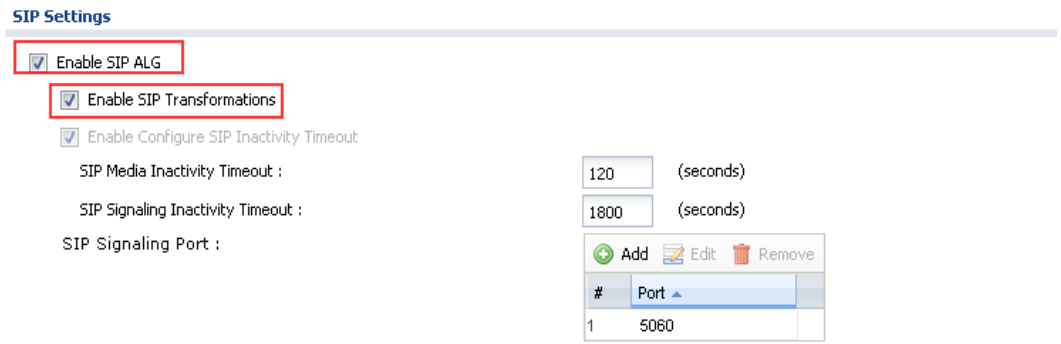
7.2 Configuration Guide

Network Conditions:

- WAN download bandwidth: 2M
- WAN upload bandwidth: 1M

Goal to achieve:

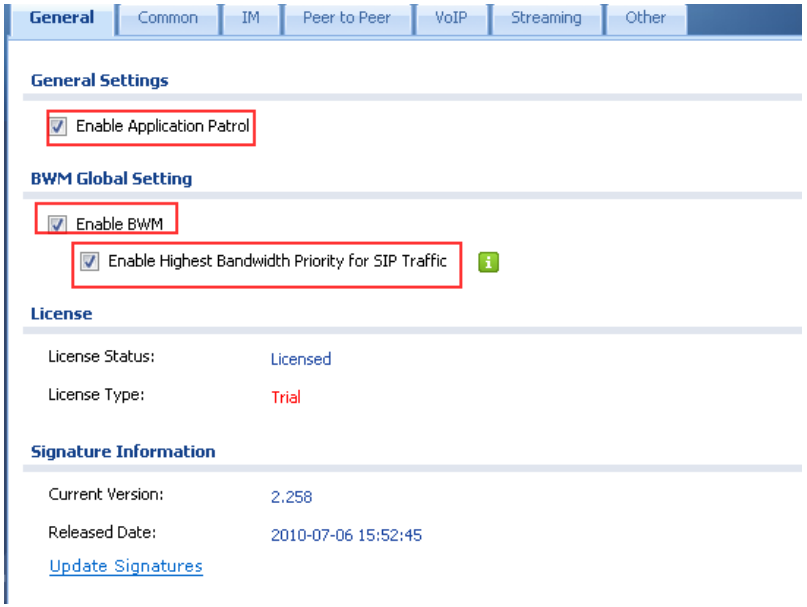
Make sure VoIP traffic has the highest priority over all other traffic.

ZLD configuration	ZyNOS configuration
<< ZyWALL USG50 configuration steps >> Step 1. Go to **Configuration > Network > ALG**, enable SIP ALG.  	Step 1. Go to **Advanced > ALG**, enable SIP ALG. (If you want to use BWM to manage VoIP traffic, SIP ALG must be enabled.)

All contents copyright (c) 2010 ZyXEL Communications Corporation.

Step 2. Go to **Configuration > App Patrol > General**, enable **Application Patrol**, enable **BWM** and enable **Highest Bandwidth Priority for SIP Traffic**.

Enabling **Highest Bandwidth Priority for SIP Traffic** forces the device to give SIP traffic the highest bandwidth priority. When this option is enabled the system ignores the bandwidth management settings of all application patrol rules for SIP traffic and does not record SIP traffic bandwidth usage statistics.



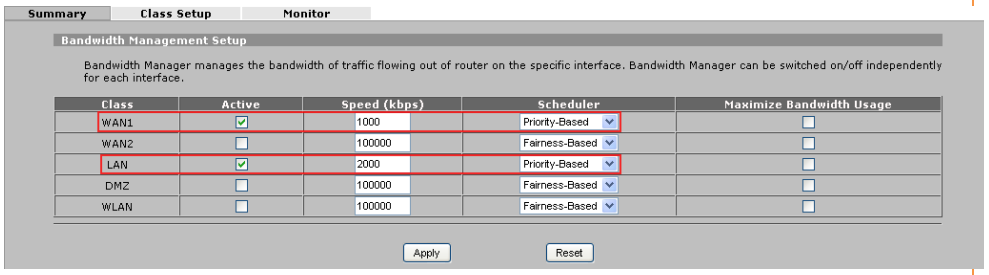
NOTE: You need to register IDP/App Patrol license to use App Patrol.

Step 2. Go to **Advanced > BW Management > Summary**.

Enable WAN1 interface. Since ISP upload speed is 1 Mbps, set WAN1 speed to 1000 kbps.

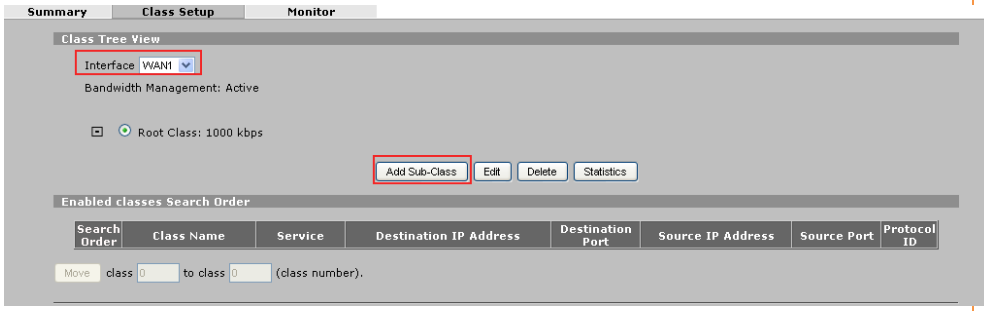
Choose **Priority-Based Scheduler**.

Enable LAN interface. Since ISP download speed is 2 Mbps, set LAN speed to 2000 kbps.



Step3. Go to **Advanced > BW Management > Class Setup**.

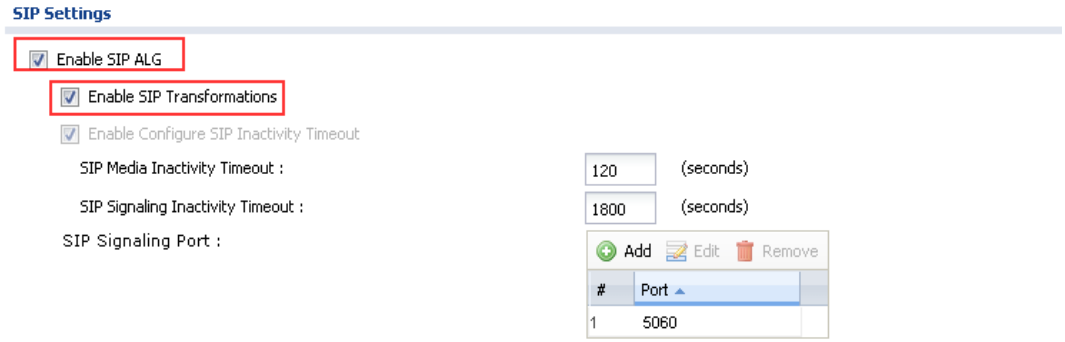
Add Sub-Class under interface WAN1 to manage upload traffic.



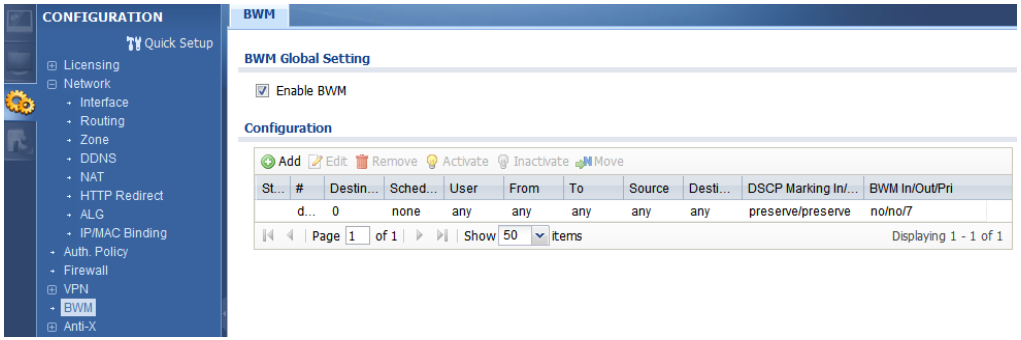
All contents copyright (c) 2010 ZyXEL Communications Corporation.

<< ZyWALL USG20/20W configuration steps >>

Step 1. Go to **Configuration > Network > ALG**, enable **SIP ALG**.



Step 2. Go to **Configuration > BWM**, enable **BWM**.



Upload bandwidth budget: 300kbps.

Priority: 7.

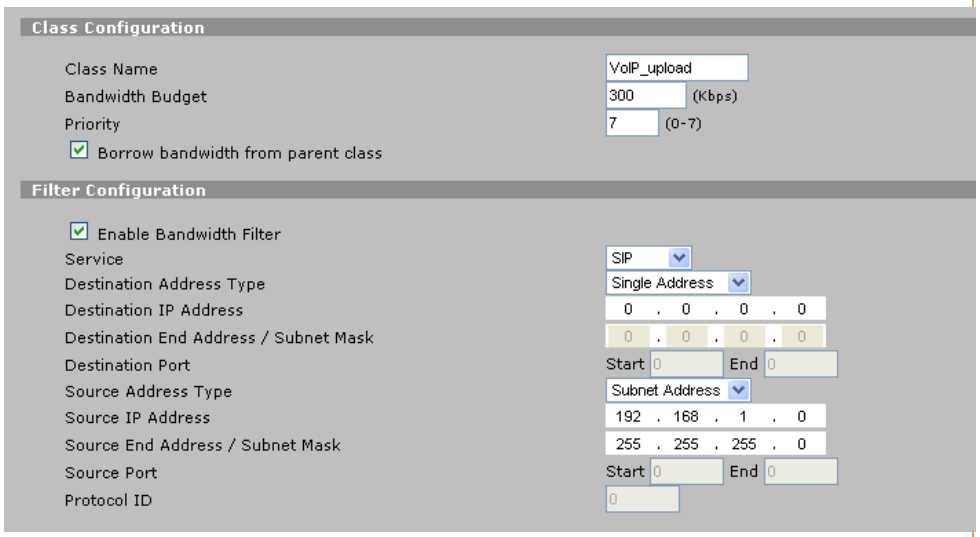
(Priority order: 7~1 — Highest ~ Lowest)

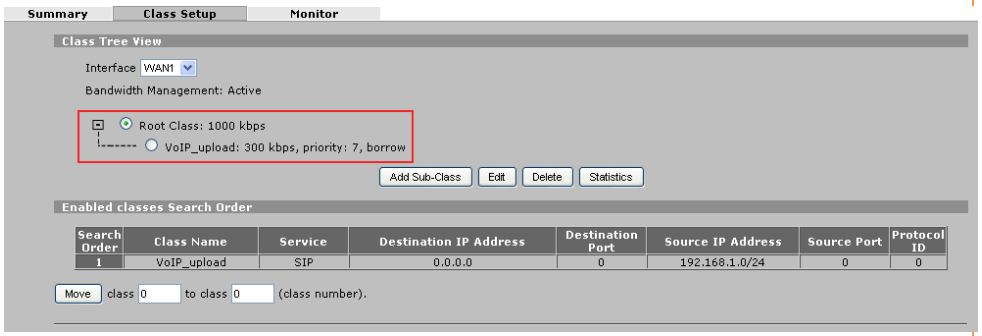
Enable Bandwidth Filter.

Service: SIP

Destination: Any

Source: LAN subnet

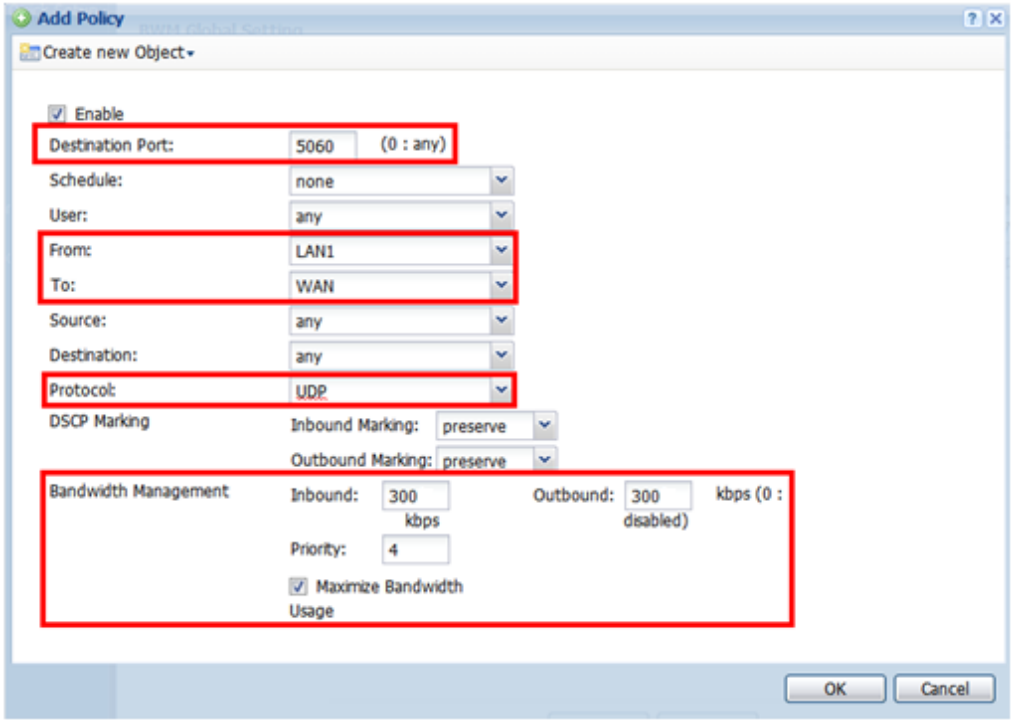




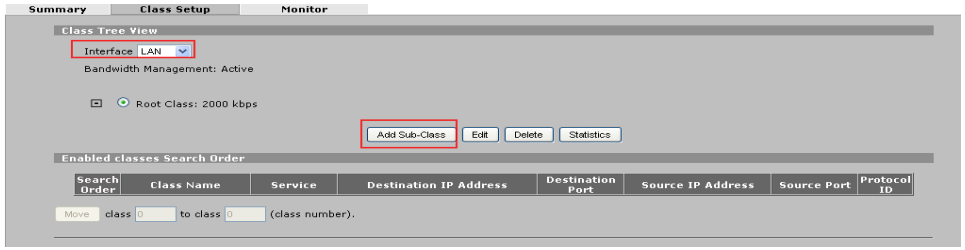
All contents copyright (c) 2010 ZyXEL Communications Corporation.

Step3. Create a bandwidth management rule and configure

- **Destination port** 5060 for SIP application
- Configure the rule as **from LAN1 to WAN**
- Select the **UDP** protocol
- Allocate 300kbps for both inbound/outbound bandwidths.



Add Sub-Class under interface LAN to manage download traffic.



To guarantee voice quality, the bandwidth for VoIP traffic with should be at least 300Kbps in both download and upload directions.

Download bandwidth budget: 300kbps.

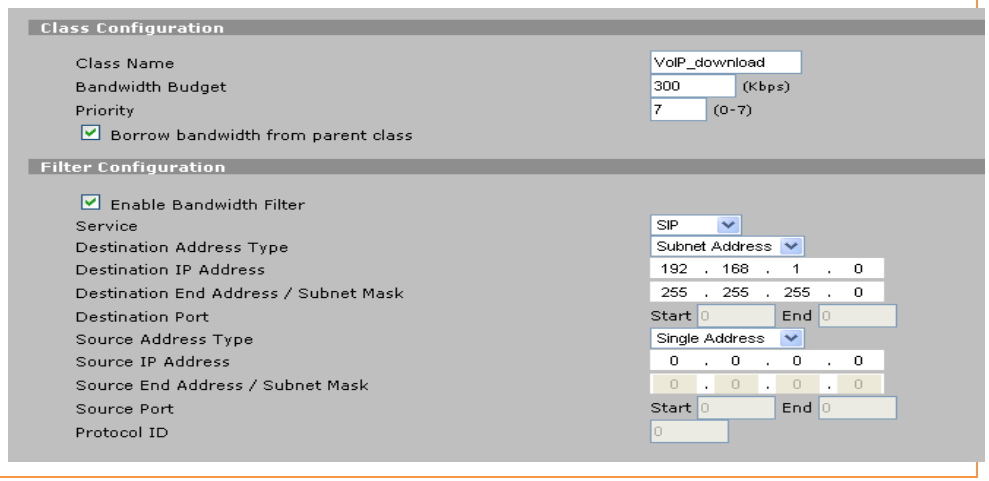
Priority: 7. (Priority order: 7~1 — Highest ~ Lowest)

Enable Bandwidth Filter.

Service: SIP

Destination: LAN subnet

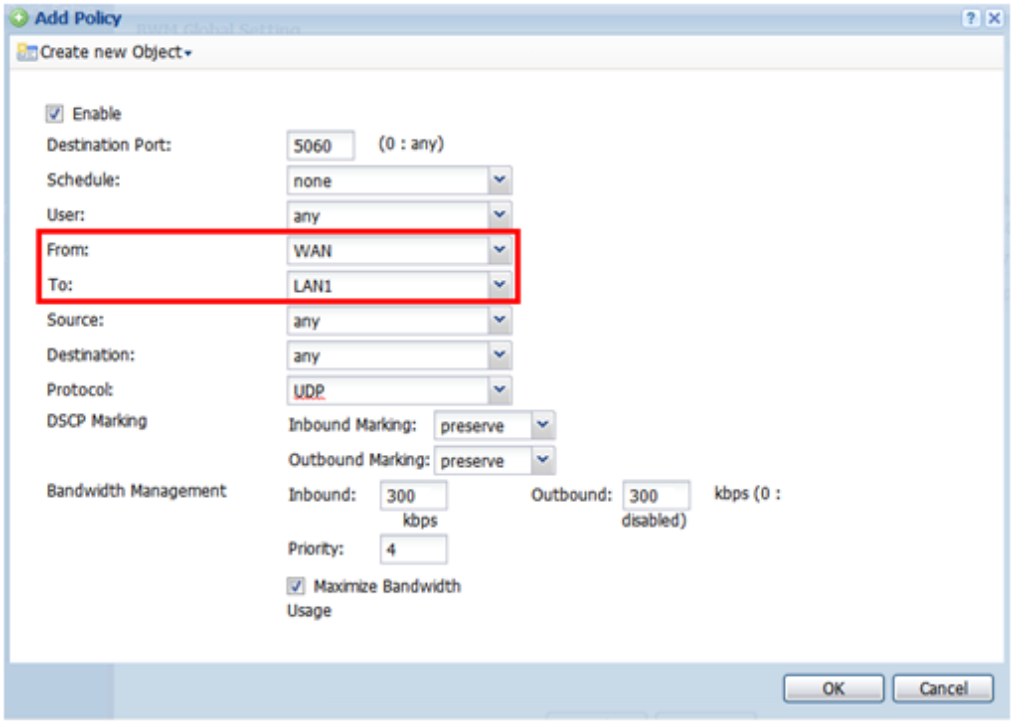
Source: Any


Class Configuration
Class Name VoIP_download
Bandwidth Budget 300 (Kbps)
Priority 7 (0-7)
Borrow bandwidth from parent class
Filter Configuration
Enable Bandwidth Filter
Service SIP
Destination Address Type Subnet Address
Destination IP Address 192 . 168 . 1 . 0
Destination End Address / Subnet Mask 255 . 255 . 255 . 0
Destination Port Start 0 End 0
Source Address Type Single Address
Source IP Address 0 . 0 . 0 . 0
Source End Address / Subnet Mask 0 . 0 . 0 . 0
Source Port Start 0 End 0
Protocol ID 0

All contents copyright (c) 2010 ZyXEL Communications Corporation.

Step4. Create a bandwidth management rule and configure

- Configure the rule as **from WAN to LAN1**
- Configure the rest identically to the above rule

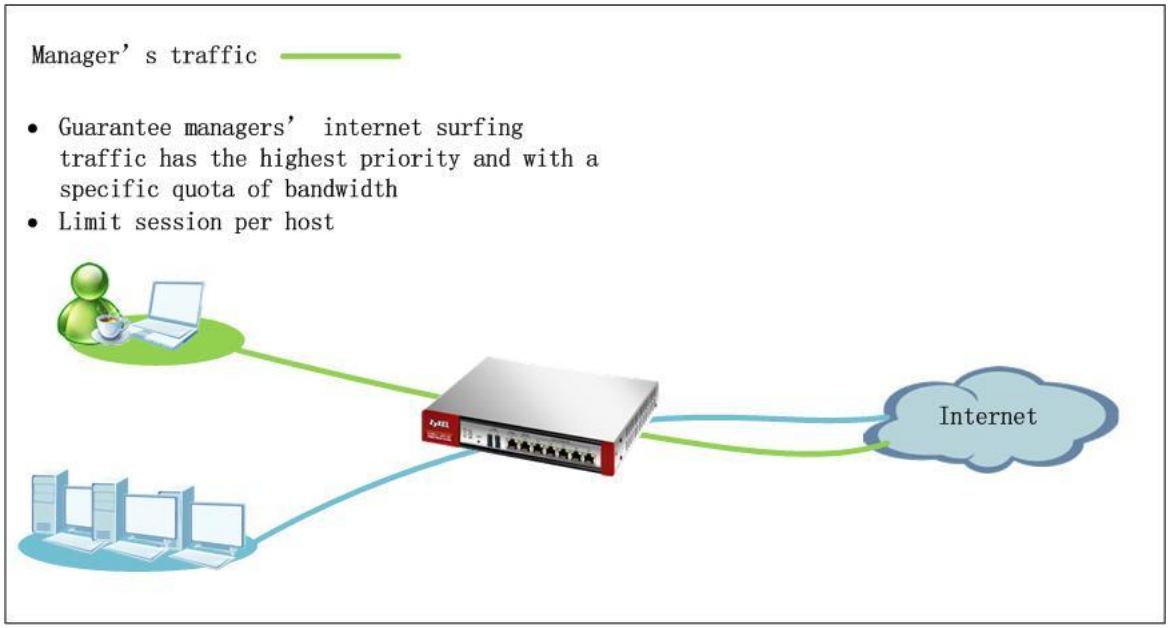


All contents copyright (c) 2010 ZyXEL Communications Corporation.

Scenario 8 — Reserving Highest Bandwidth Management Priority for a Superior User and Control Session per Host

8.1 Application Scenario

Among all the traffic in the company network, sometimes we need to assign higher priority to some superior users to keep their important work going on smoothly. For example, the general manager needs to surf Internet smoothly to conduct his daily important work. Therefore, the network administrator should use the bandwidth management function to prioritize the manager's Internet traffic, and guarantee a minimum bandwidth for his traffic.
During the office hours, to prevent any user consuming too much of the company's bandwidth, the network administrator should limit the number of sessions each user may use.


Manager' s traffic
Guarantee managers' internet surfing traffic has the highest priority and with a specific quota of bandwidth
Limit session per host
Internet

All contents copyright (c) 2010 ZyXEL Communications Corporation.

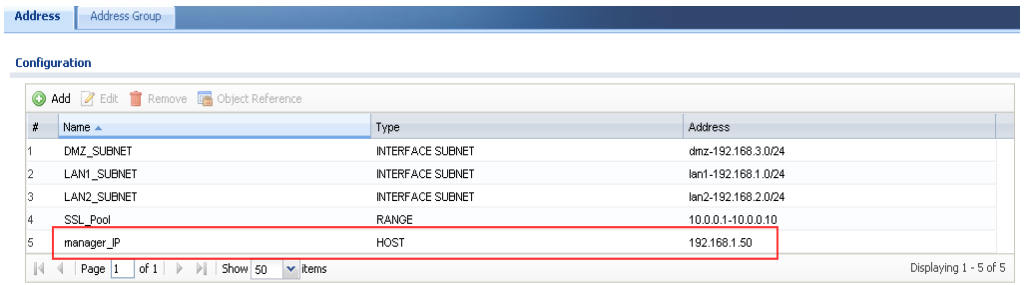
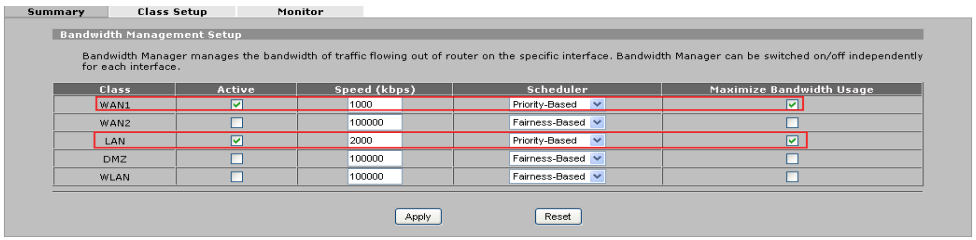
8.2 Configuration Guide

Network Conditions:

- WAN download bandwidth: 2M
- WAN upload bandwidth: 1M
- Manager's PC IP: 192.168.1.50

Goal to achieve:

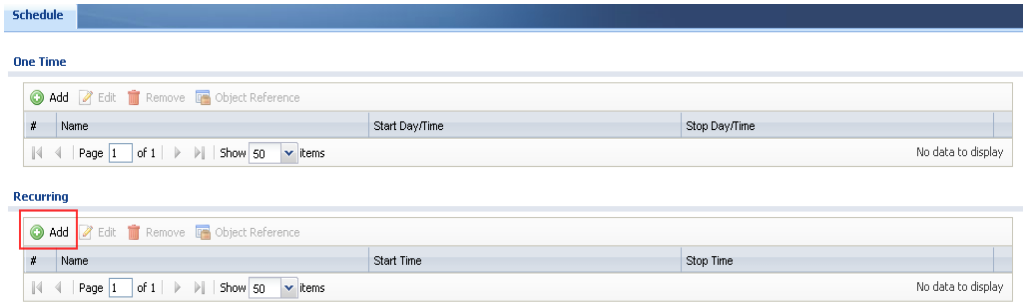
Guarantee manager's internet surfing traffic going smoothly. Limit each user's session numbers to prevent any user from using up too many sessions.

ZLD configuration	ZyNOS configuration
<< ZyWALL USG50 configuration steps >> Step 1. Go to **Configuration > Object > Address**, add an address object for the manager. manager_IP: 192.168.1.50 	Step 1. Go to **ADVANCED > BW MGMT > Summary**. Enable **BWM** on WAN1. Set the **speed** to 1000kbps (upload bandwidth). Set the scheduler to **Priority-Based**. Enable **Maximize Bandwidth Usage**. Enable **BWM** on LAN. Set **speed** to 2000kbps (download bandwidth). Set the scheduler to **Priority-Based**. Enable **Maximize Bandwidth Usage**. 

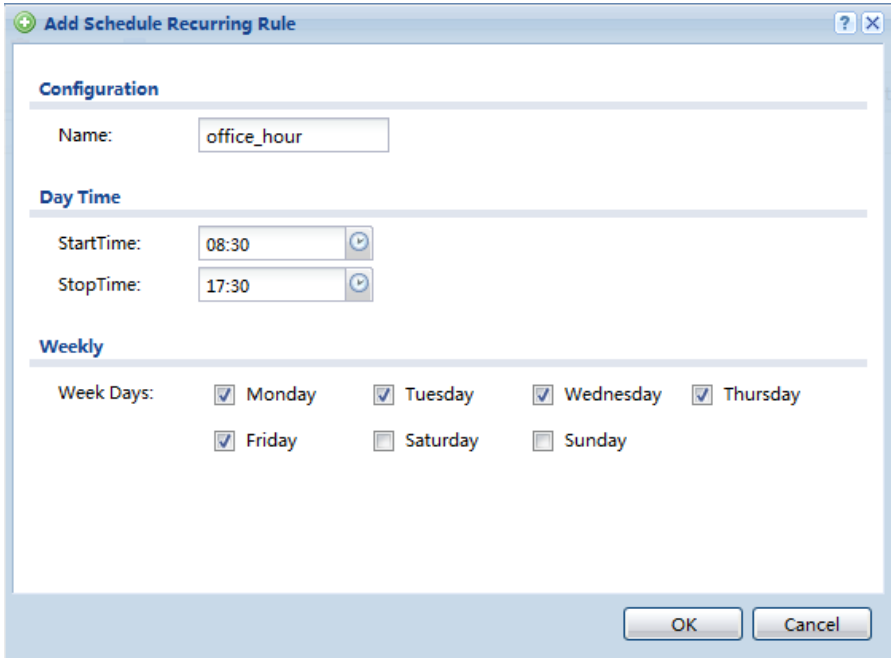
Summary
Class Setup
Monitor
Bandwidth Management Setup
Bandwidth Manager manages the bandwidth of traffic flowing out of router on the specific interface. Bandwidth Manager can be switched on/off independently for each interface.
Class Active Speed (kbps) Scheduler Maximize Bandwidth Usage
WAN1 1000 Priority-Based
WAN2 100000 Fairness-Based
LAN 2000 Priority-Based
DMZ 100000 Fairness-Based
WLAN 100000 Fairness-Based
Apply
Reset

All contents copyright (c) 2010 ZyXEL Communications Corporation.

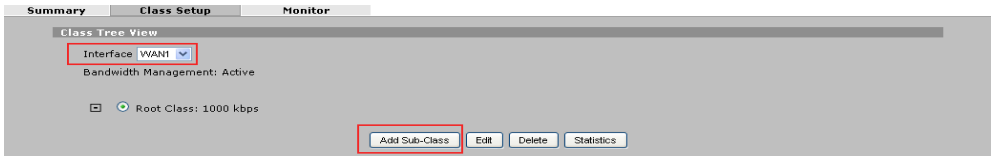
Step 2. Go to **Configuration > Object > Schedule**. Add one recurring schedule object.



Input **Start Time** and **Stop Time**, and choose the **weekdays**.



Step 2. Go to **ADVANCED > BW MGMT > Class Setup**. Choose WAN1 to configure upload bandwidth management. Add a Sub-Class.



Bandwidth Budget: Allocate 100kbps for the manager's http upload traffic.

Priority: Assign the highest priority 7.

Enable **Borrow bandwidth from parent class**.

Enable **Bandwidth Filter**

Service: choose **Custom**

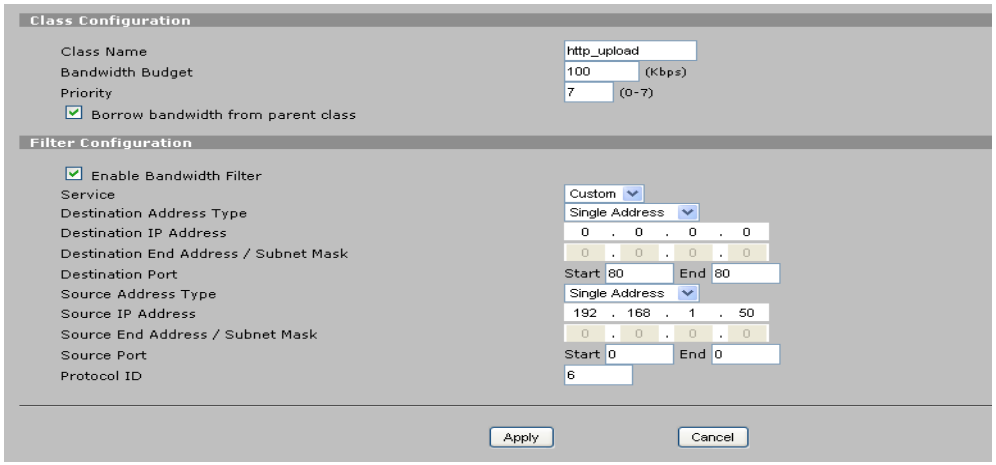
Destination Address: **Any**

Destination Port: **80(HTTP)**

Source Address: **manager's IP 192.168.1.50**

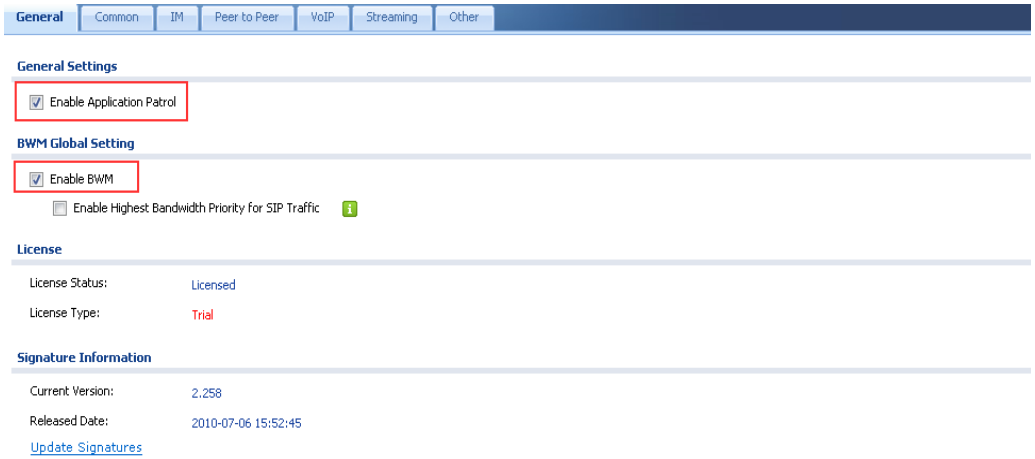
Source Port: **Any**

Protocol ID: **6(TCP)**

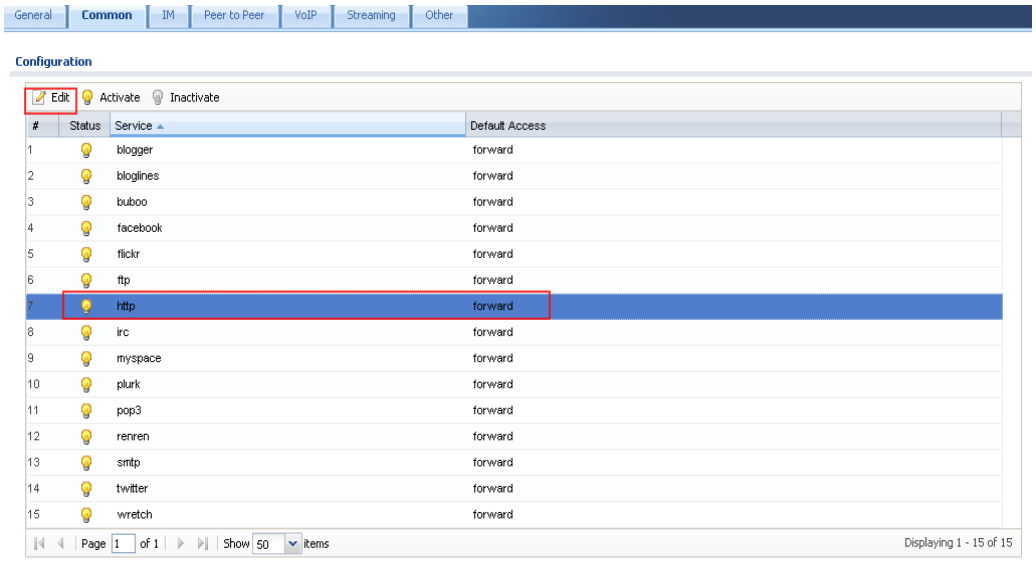


All contents copyright (c) 2010 ZyXEL Communications Corporation.

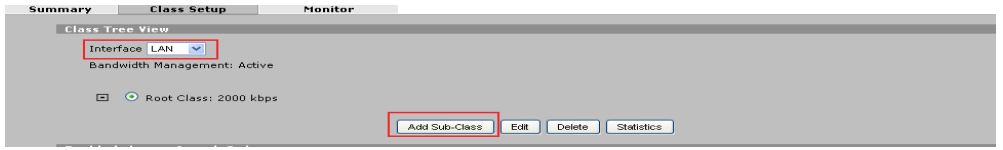
Step3. Go to **Configuration > App Patrol > General**. Enable Application Patrol, and enable BWM.



Step4. **Configuration > App Patrol > Common**. Edit the application "**http**".



Step3. Go to **ADVANCED > BW MGMT > Class** Setup. Choose LAN to configure download bandwidth management. Add a Sub-Class.



Bandwidth Budget: Allocate 300kbps for the manager's http download traffic.

Priority: Assign the highest priority 7.

Enable **Borrow bandwidth from parent class.**

Enable **Bandwidth Filter**

Service: choose **Custom**

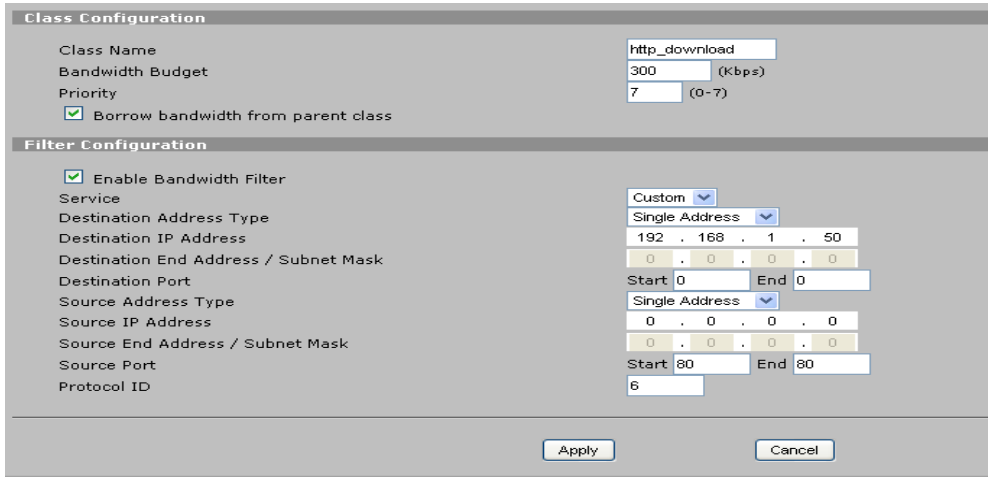
Destination Address: **manager's IP 192.168.1.50**

Destination Port: **Any**

Source Address: **Any**

Source Port: **80(HTTP)**

Protocol ID: **6(TCP)**



All contents copyright (c) 2010 ZyXEL Communications Corporation.

Add a policy to manage the manager's http traffic bandwidth.

Direction: from LAN to Any.

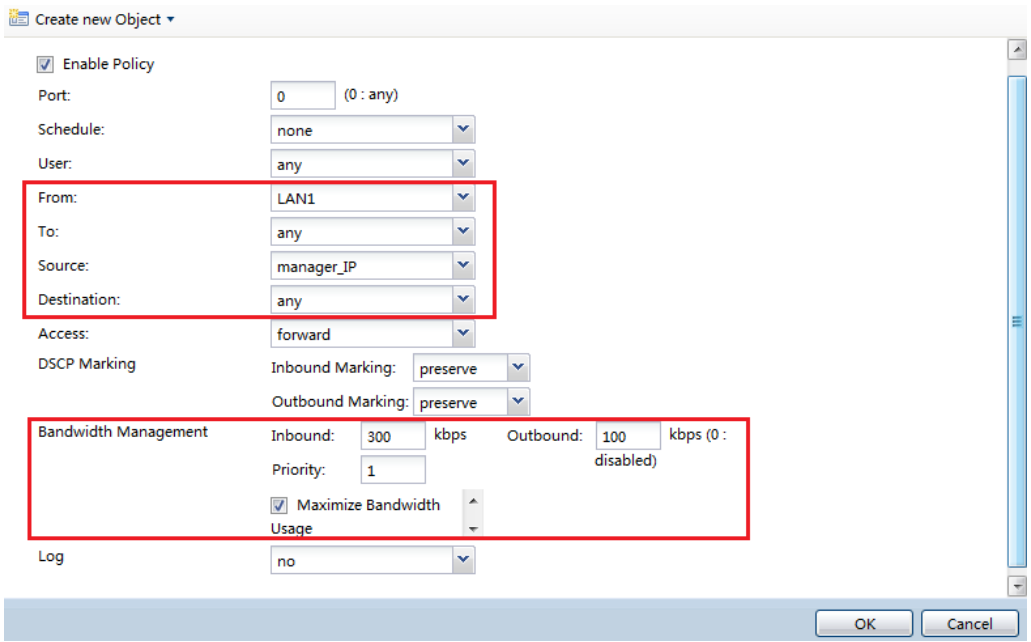
Source: manager_IP

Destination: any

Bandwidth Management: To guarantee the manager can surf internet smoothly, we can assign a bandwidth of 300kbps for inbound traffic (download), and assign a bandwidth of 100kbps for outbound traffic (upload). For the definition of Inbound and Outbound, please refer to the App Patrol BWM Direction NOTE below.

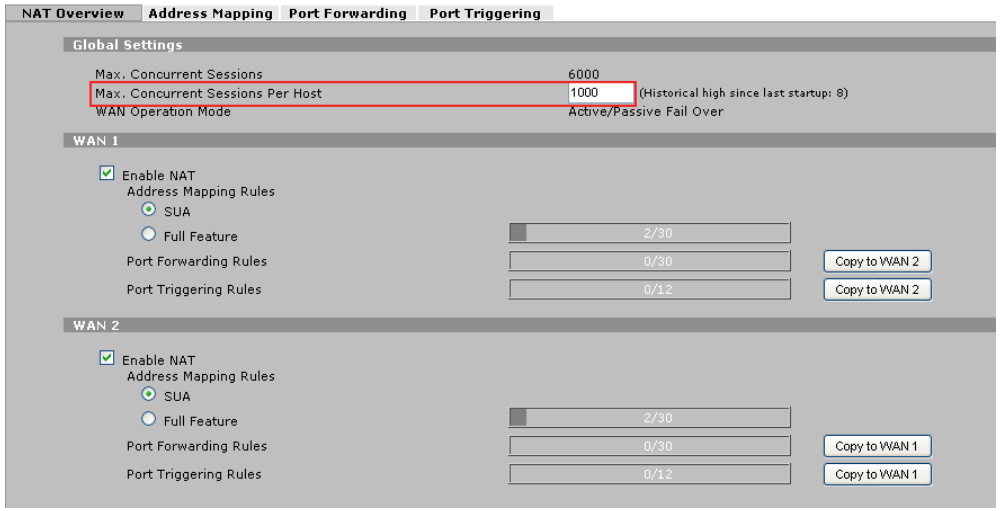
Set priority as the highest —**1**.

Enable **Maximize Bandwidth Usage**.



Limit each user's number of sessions

To prevent any user from consuming too many sessions, we can limit each user's sessions to a specific number. Go to ADVANCED > NAT > NAT Overview. Set Max. Concurrent Sessions Per Host to 1000. Administrator can adjust this value according to his real network environment.



All contents copyright (c) 2010 ZyXEL Communications Corporation.

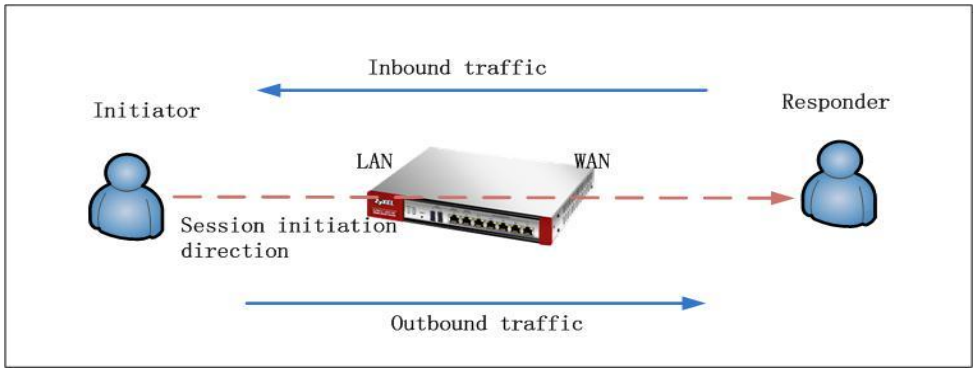
App Patrol BWM Direction NOTE

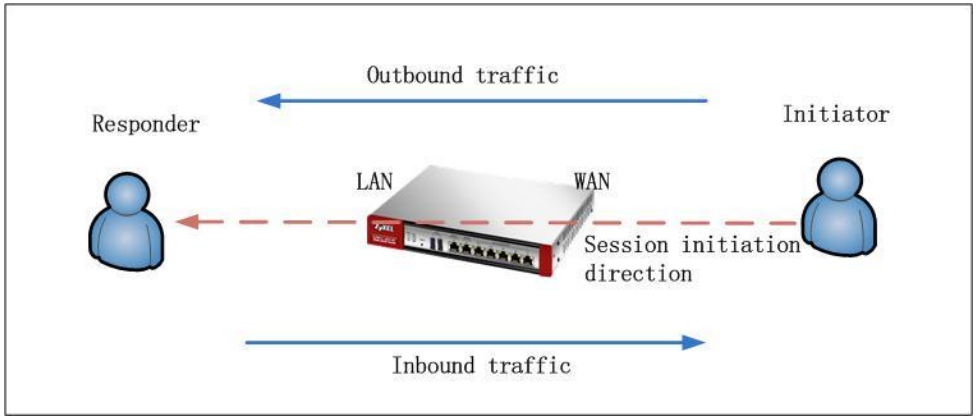
To use App Patrol to manage bandwidth correctly, users must understand the direction Inbound and Outbound.

The direction Inbound and Outbound are determined with the traffic session initiation direction as reference.

Inbound: From session responder to session initiator

Outbound: From session initiator to session responder.

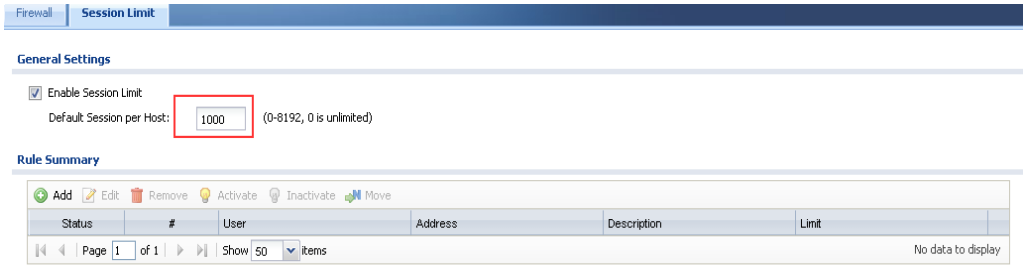




All contents copyright (c) 2010 ZyXEL Communications Corporation.

Limit each user's session number

To prevent any user from using up too many sessions, we can limit each user's sessions to a specific number. Go to **Configuration > Firewall > Session Limit**. Enable **Session Limit**, and set **Default Session per Host** to 1000. Administrator can adjust this value according to his real network environment.

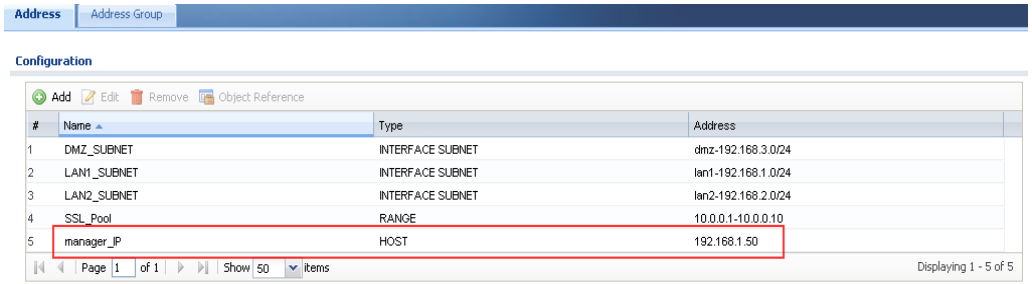


All contents copyright (c) 2010 ZyXEL Communications Corporation.

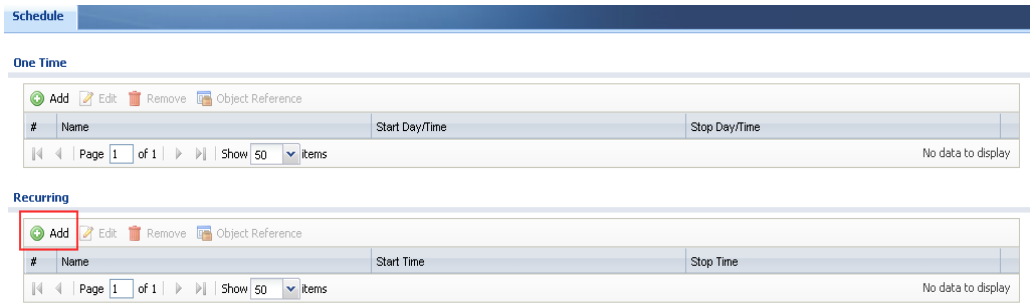
<< ZyWALL USG20/20W configuration steps >>

Step 1. Go to **Configuration > Object > Address**, Add an address object for the manager.

manager_IP: 192.168.1.50

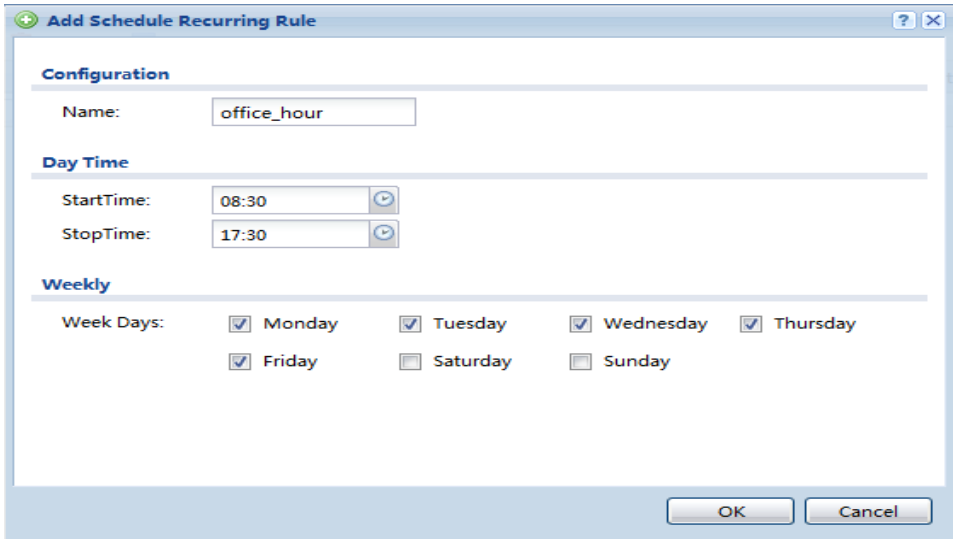


Step 2. Go to **Configuration > Object > Schedule**. Add one recurring schedule object.



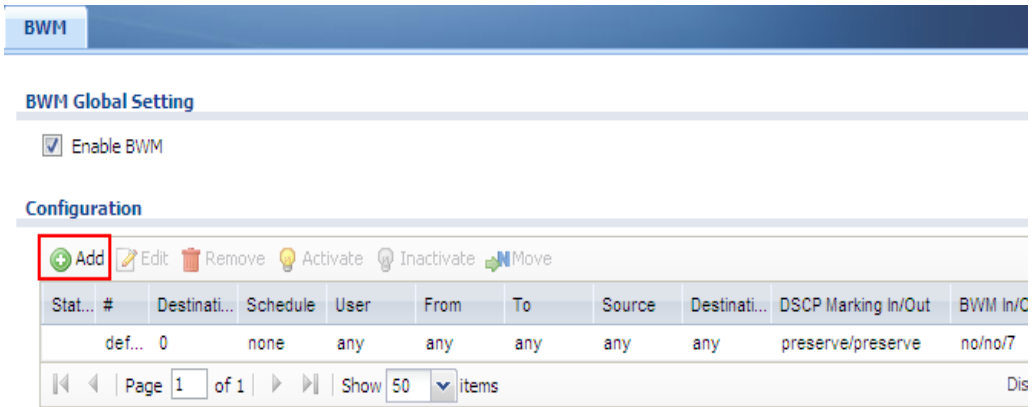
All contents copyright (c) 2010 ZyXEL Communications Corporation.

Input **Start Time** and **Stop Time**, and choose the **weekdays**.



Step3. Go to **Configuration > BWM**.

Add a policy to manage the manager's http traffic bandwidth.



All contents copyright (c) 2010 ZyXEL Communications Corporation.

Destination Port: 80

Schedule: the recurring schedule object configured in step2.

Direction: from LAN1 to WAN.

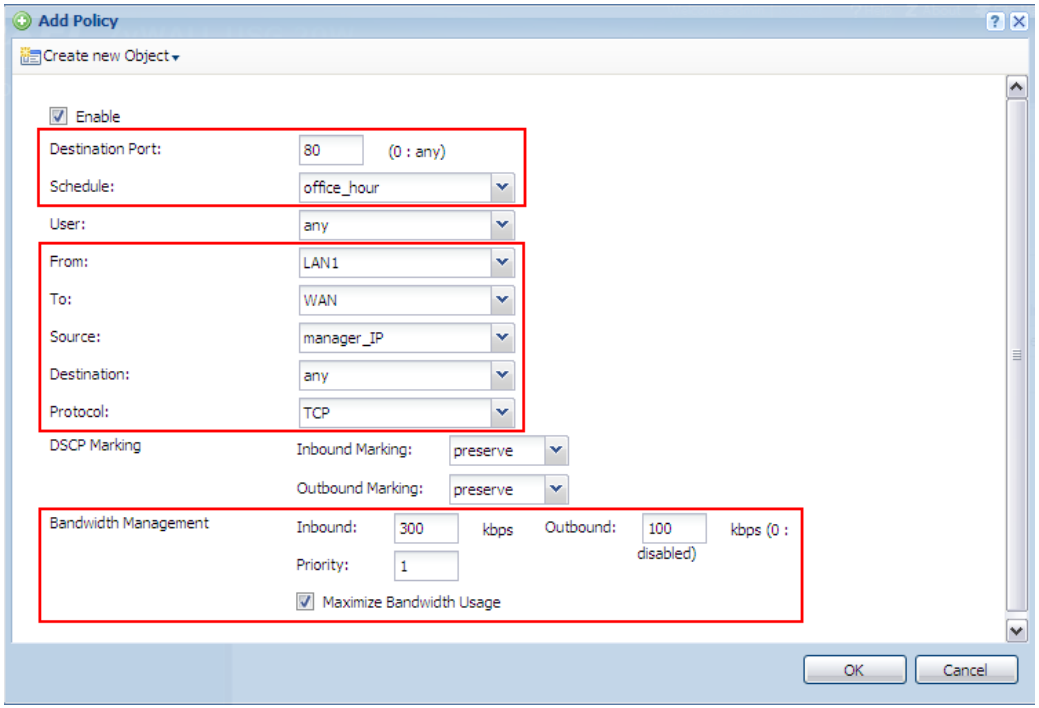
Source: manager_IP

Destination: any

Protocol: TCP

Bandwidth Management: To guarantee the manager can surf internet smoothly, we can assign a bandwidth of 300kbps for inbound traffic (download), and assign a bandwidth of 100kbps for outbound traffic (upload). Set priority as the highest 1.

Enable **Maximize Bandwidth Usage**.

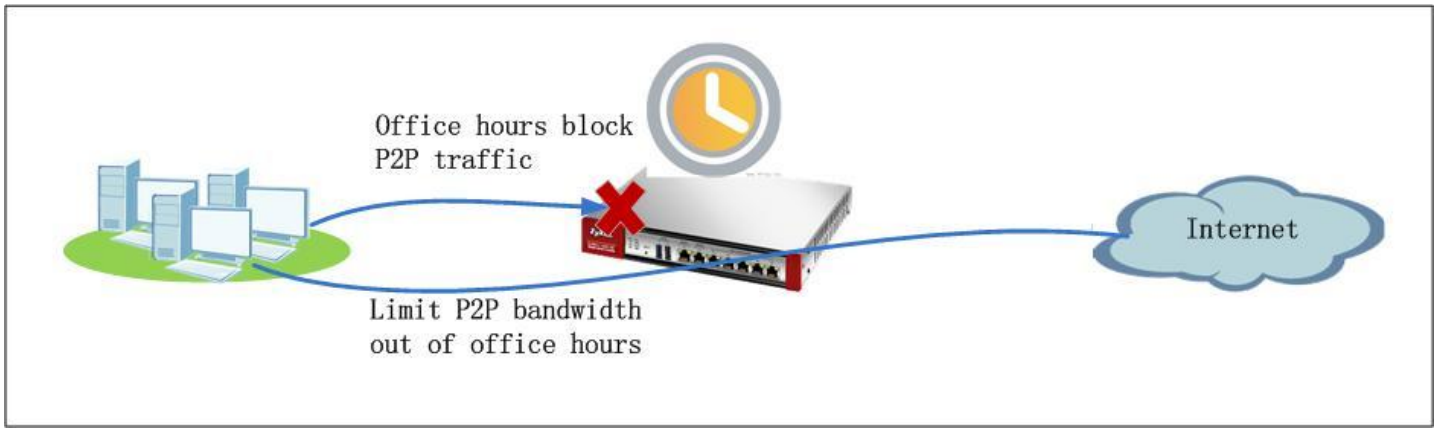


All contents copyright (c) 2010 ZyXEL Communications Corporation.

Scenario 9 — Using ZyWALL to Control Popular P2P Applications

9.1 Application Scenario

Peer to Peer applications, with their massive numbers of concurrent sessions and fast traffic transmission speed, can consume much of a company's limited bandwidth. This will slow down other normal productive traffic speed and affect productivity, lowering company productivity profit. USG ZyWALL's Application Patrol function can examine passing traffic in real time, detect traffic service type, and take corresponding actions according to the configuration in App Patrol. For example, to improve network productivity efficiency, network administrator can set App Patrol to block P2P traffic in office hours, and limit its speed with bandwidth management out of office hours.



All contents copyright (c) 2010 ZyXEL Communications Corporation.

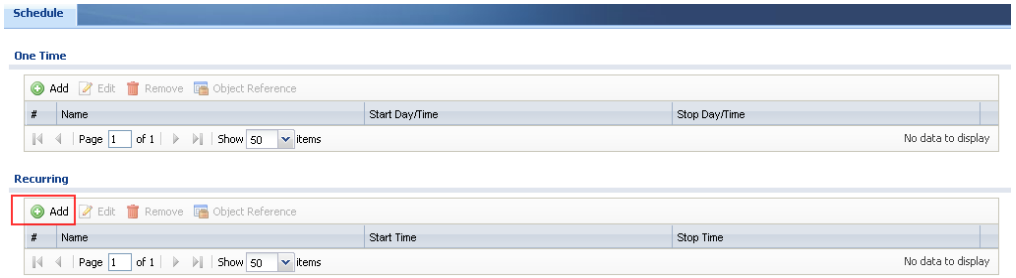
9.2 Configuration Guide

Network Conditions:

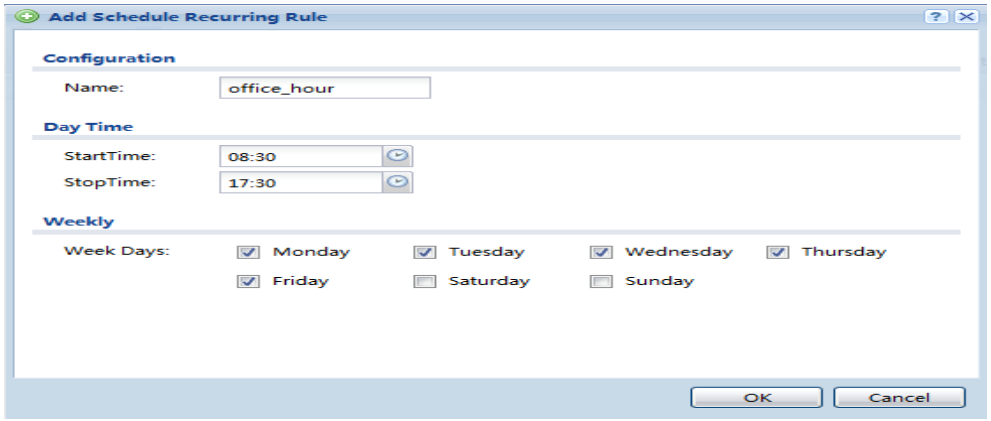
- LAN subnet: 192.168.1.0/24

Goals to achieve:

1) Block P2P traffic during office hours (8:30~17:30)
2) Allow P2P traffic out of office hours but limit its bandwidth to 100kbps.

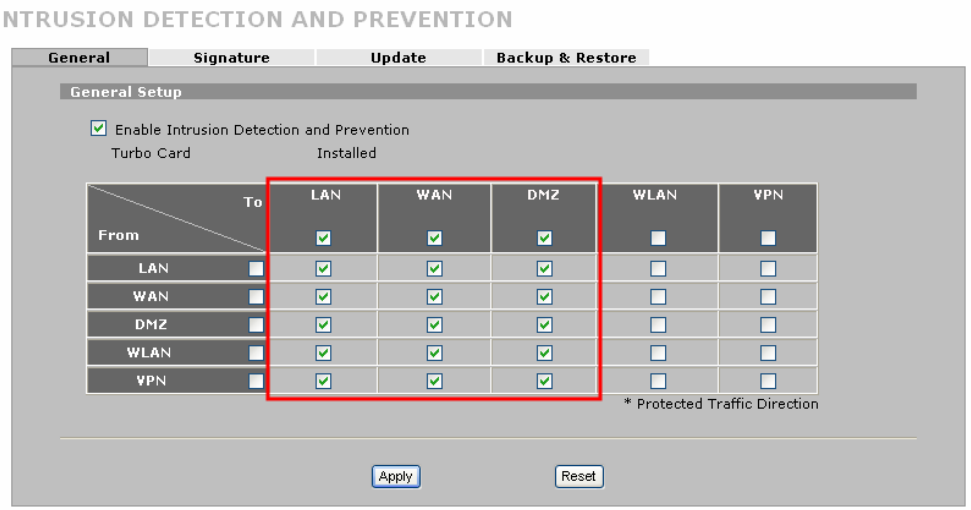
ZLD configuration	ZyNOS configuration
Step 1. Go to **Configuration > Object > Schedule**, add a Recurring schedule object for the office hours.  	Step 1. IDP Common Setting. a. In **IDP->General**, check the **Enable Intrusion Detection and Prevention** check box to enable IDP function. b. In **Active** option, check all the traffic to LAN, DMZ and WAN check boxes to have the IM/P2P traffic between LAN zone users and the remote users under control. c. Click the **Apply** button to save the above settings.

All contents copyright (c) 2010 ZyXEL Communications Corporation.



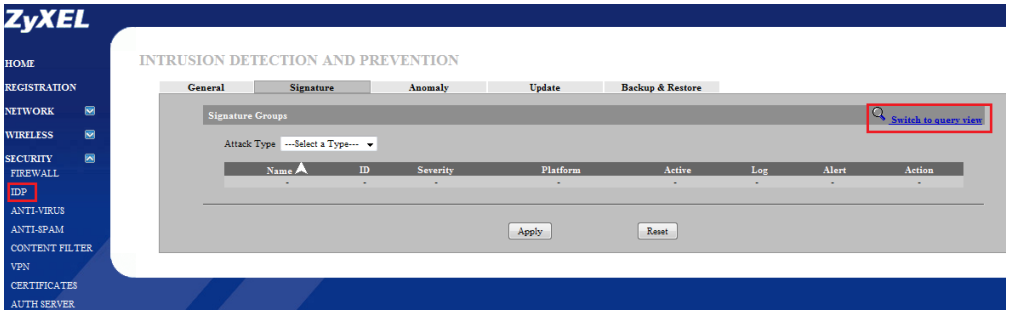
Step 2. Go to **Configuration > App Patrol > General**. First of all, please make sure you have activated your IDP/App Patrol license.

Enable **Application Patrol**, and enable **BWM**.



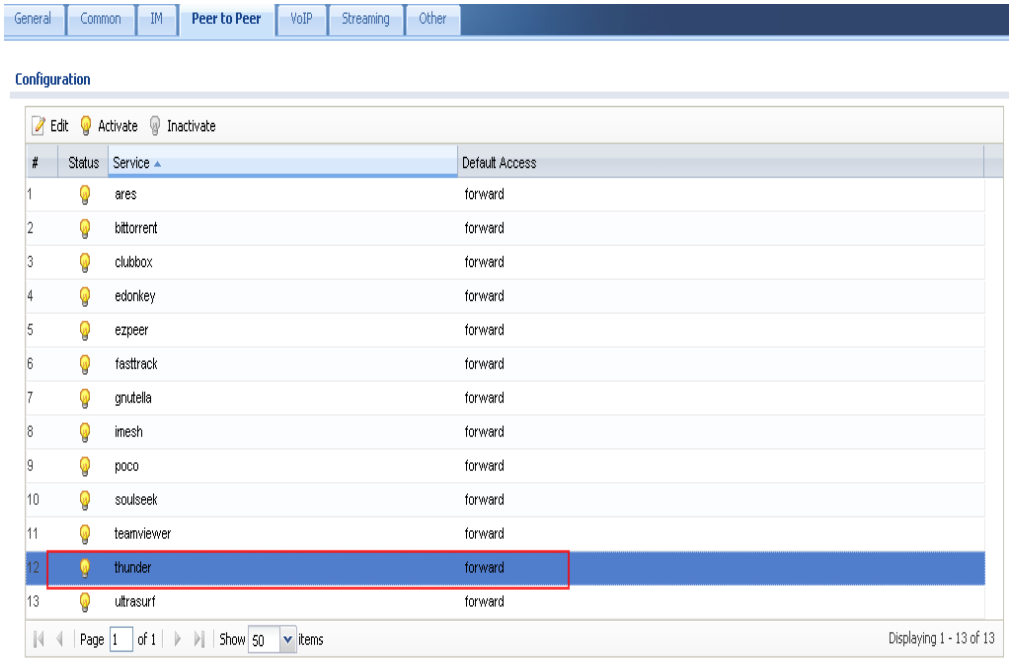
Step 2. Control Thunder application.

a. In **IDP->Signature**, click on **Switch to query view** to search for the specified signatures and set them up optionally.

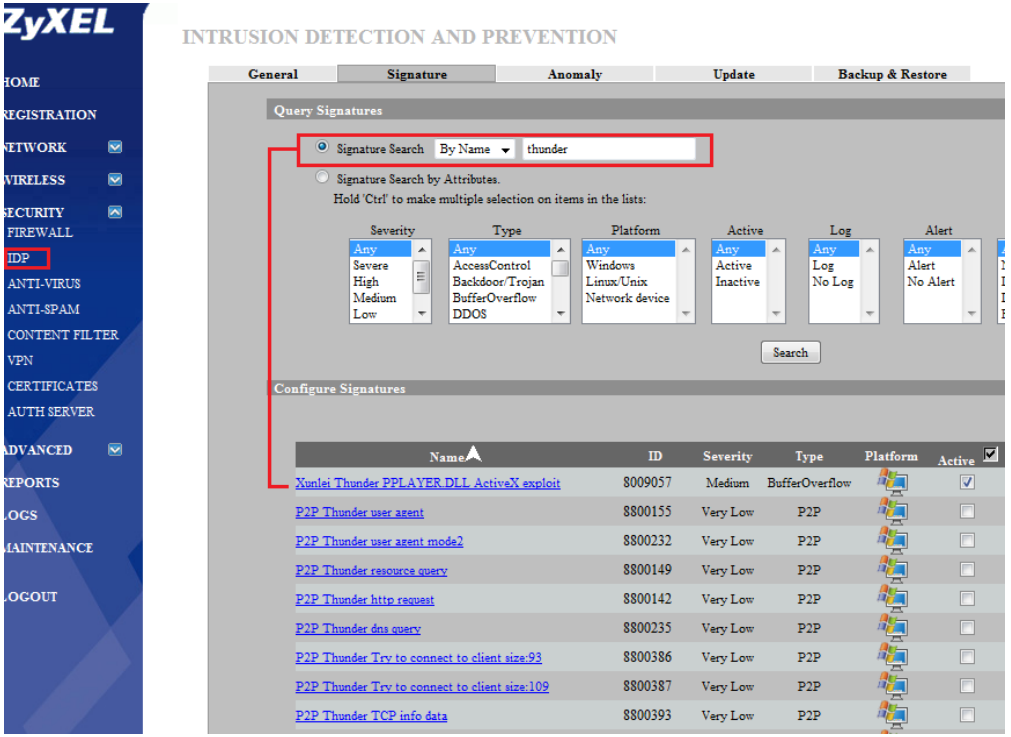


All contents copyright (c) 2010 ZyXEL Communications Corporation.

Step3. Switch to **Configuration > App Patrol > Peer to Peer**. Edit the P2P services you need to control. In this example, we will edit the thunder application.

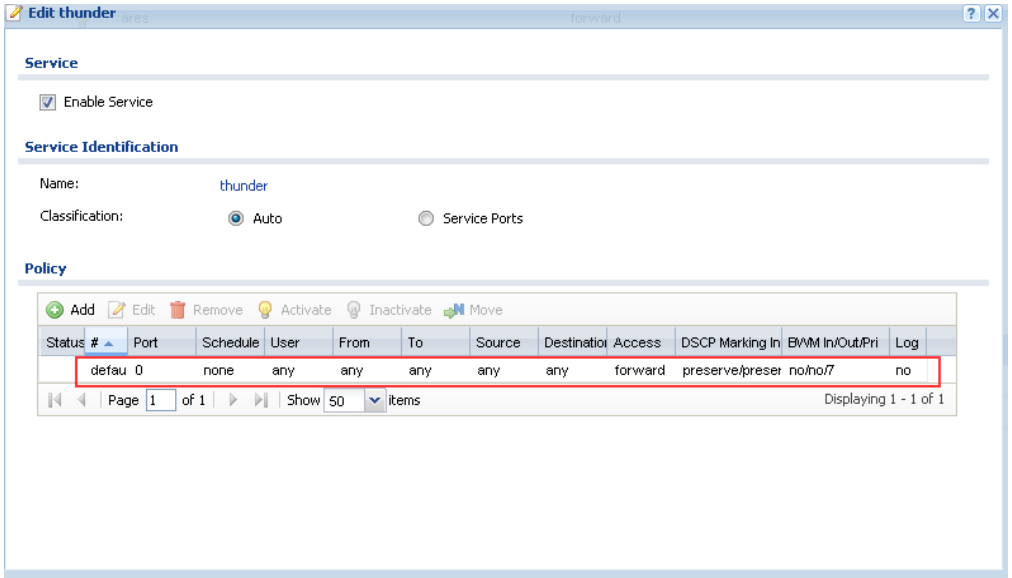


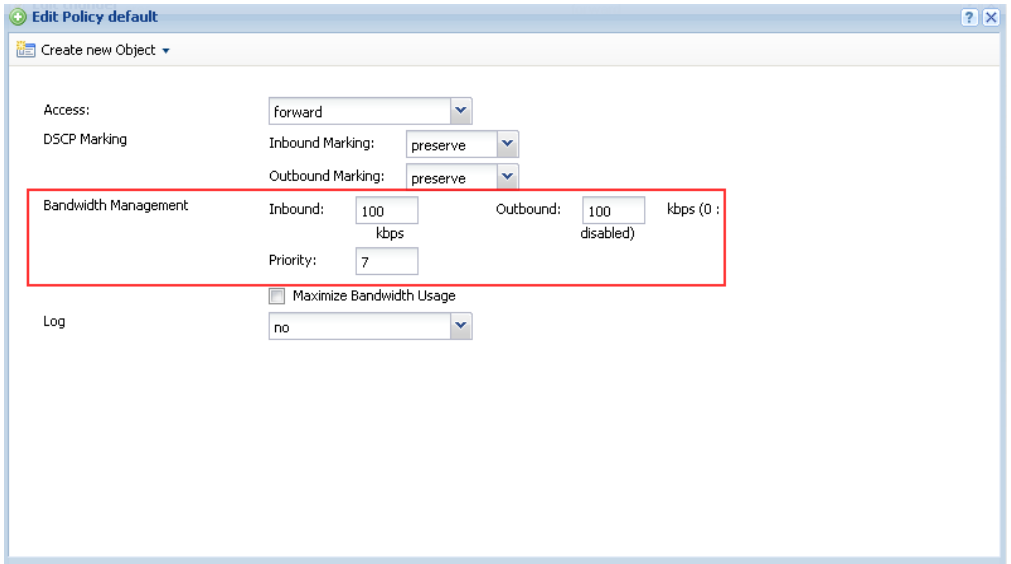
b. Use the “Thunder” keyword to search for and list any signatures related to “thunder”.



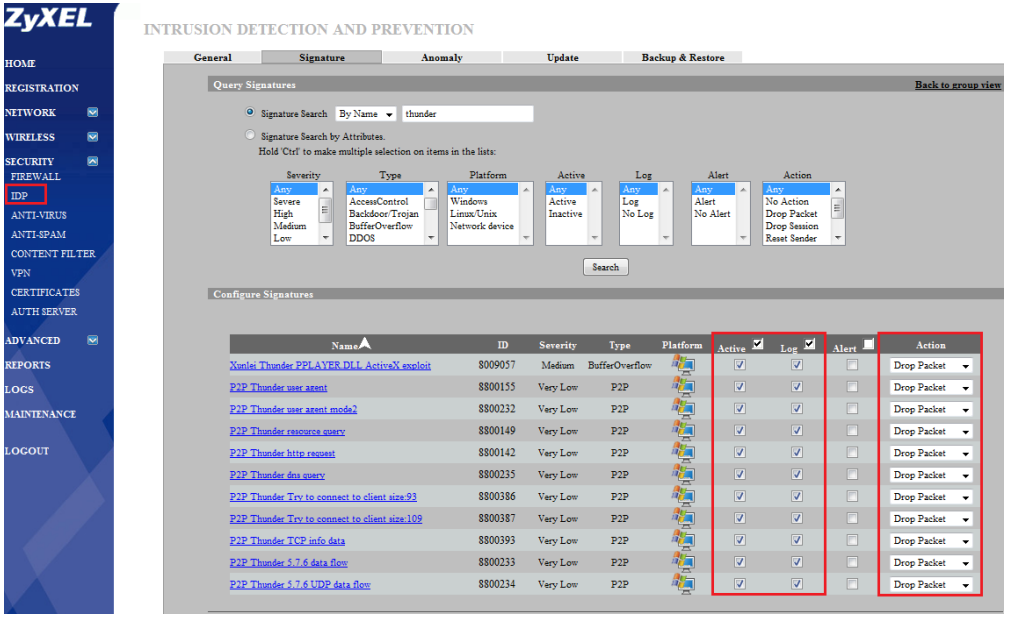
All contents copyright (c) 2010 ZyXEL Communications Corporation.

Edit the default policy. Limit its bandwidth to 100kbps for both inbound and outbound traffic. Assign the lowest priority —7 for it.





c. IT staff can log all Thunder traffic by checking the Log check box and blocking the Thunder packets by selecting **Drop Packet** in the Action field. Also remember to check the **Active** check box to activate the signatures.



All contents copyright (c) 2010 ZyXEL Communications Corporation.

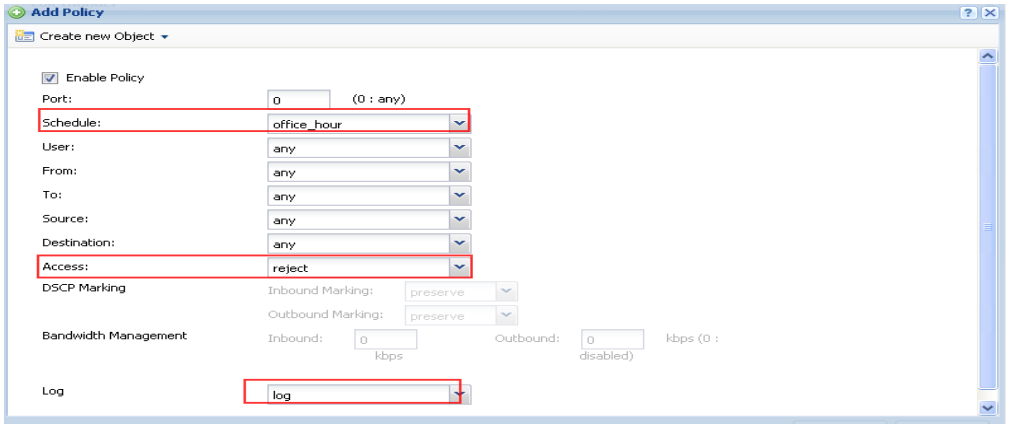
Add a policy to block thunder traffic during office hours.

Schedule: Choose the object **office_hour**

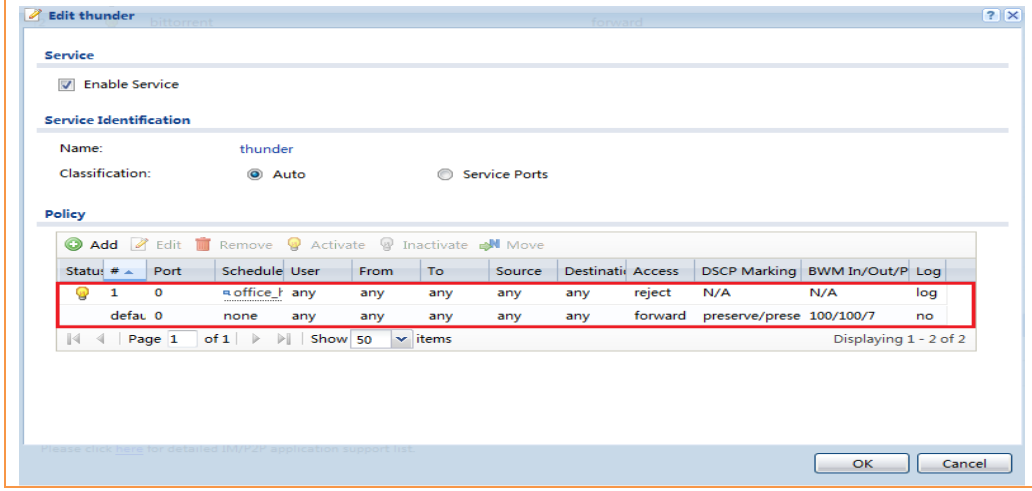
Session direction: from Any to Any

Access: Reject

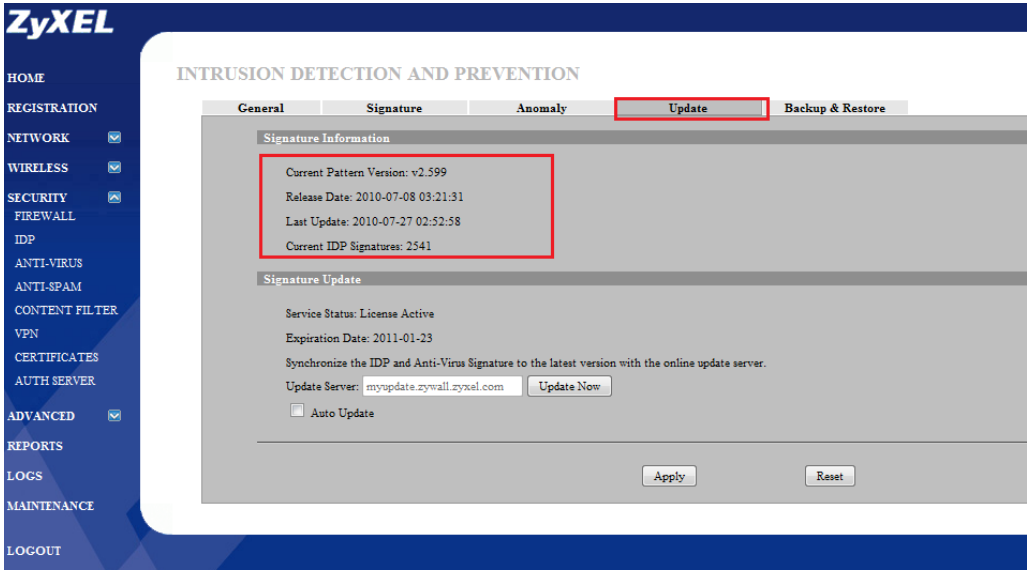
We can enable Log to check which user tries to violate the rule.



Check the created policies. Make sure their order lists as below:



Step 3. IDP signature update. To keep the ZyWALL IDP engine performing at its best, make sure the IDP signatures are kept updated (The **update** procedure can be done manually or automatically.)



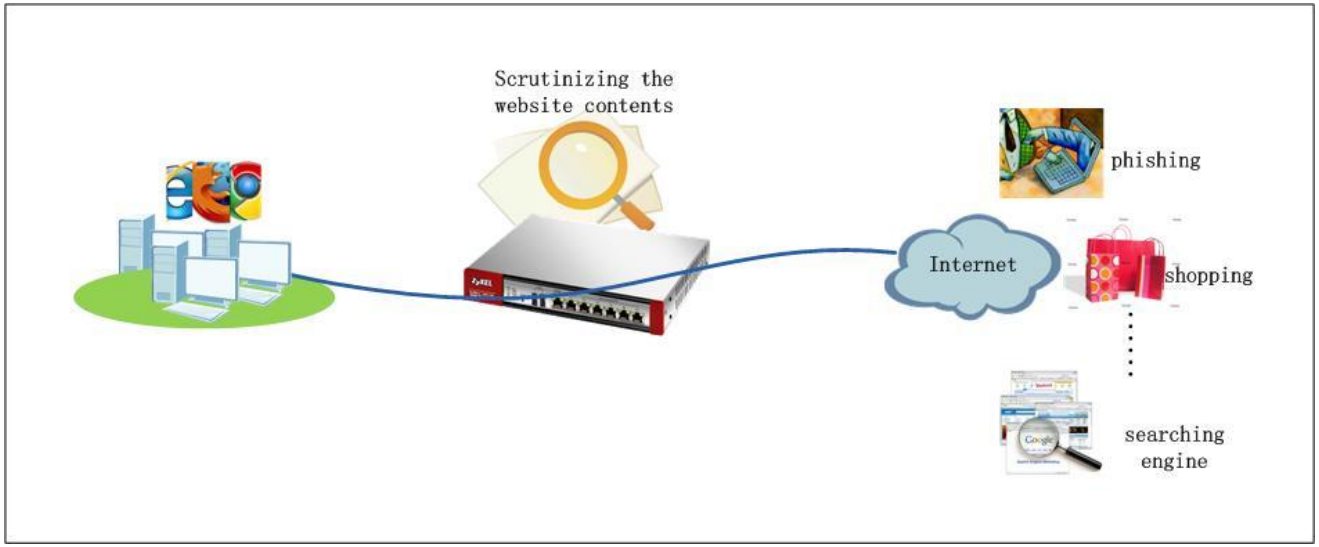
NOTE: You need to register an IDP license to use the IDP function.

All contents copyright (c) 2010 ZyXEL Communications Corporation.

Scenario 10 — Deploying Content Filtering to Manage Employee Browsing Behavior

During their daily productive work for the company, working crew needs to surf the Internet to search for information to conduct their jobs. Browsing websites that are irrelevant to work is a waste of human resources as well as a waste of company network resources. There're also some unsafe websites which may contain phishing or malicious programs. These unsafe websites should also be avoided. So the network administrator needs to make policies to prevent these undesirable types of browsing.

ZyXEL Content Filtering service, including its Safe Browsing service, is tailored to help network administrator to handle these requirements.



All contents copyright (c) 2010 ZyXEL Communications Corporation.

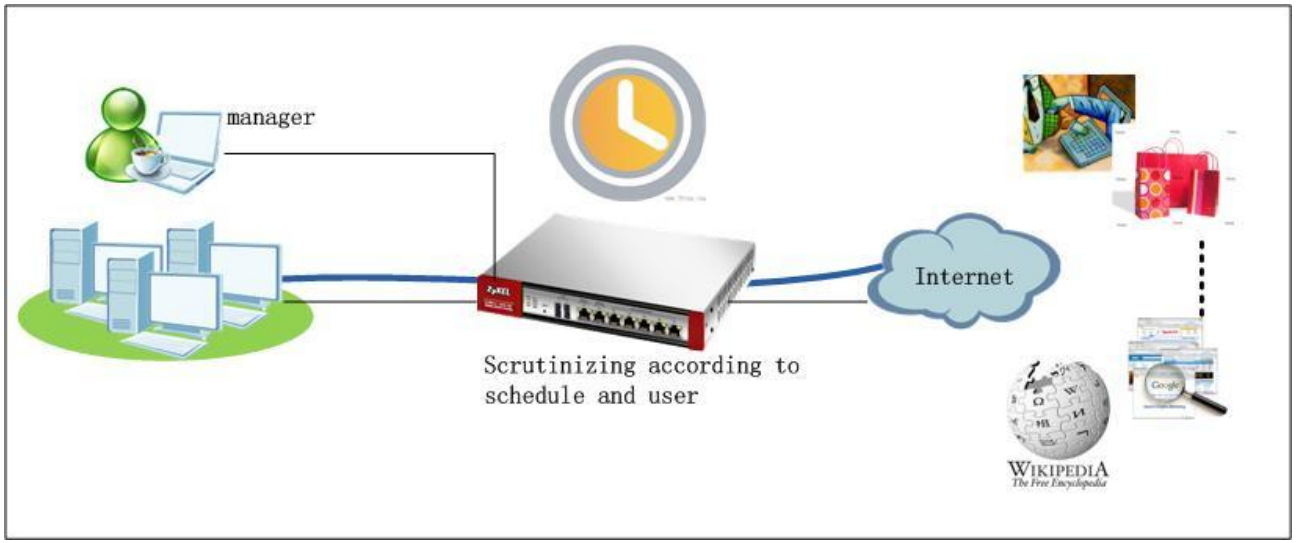
10.1 Introduction to ZSB (ZyXEL Safe Browsing)

ZSB stands for ZyXEL Safe Browsing.

As suggested by its name, this function enhances web browsing safety. With the Internet becoming more and more popular, an increasing number of threats are injected into web pages. Some web pages may be phishing web sites where the visitors may be enticed to release their confidential information, other web pages may contain malware intended to infect the visitor's PC with viruses or even to corrupt the visitor's PC. Additionally, some web pages may contain spyware sources. ZSB has been added to ZyWALL to help protect users from such unsafe web sites.

10.2 Application Scenario

During office hours, the employees should dedicate their time to their jobs and be restricted from browsing websites irrelevant to their work. But the manager should be able to access all websites without restriction at all times with the exception of unsafe websites. At other times outside of office hours, the restrictions for employees can be removed. The employees may access all websites except for unsafe websites.



All contents copyright (c) 2010 ZyXEL Communications Corporation.

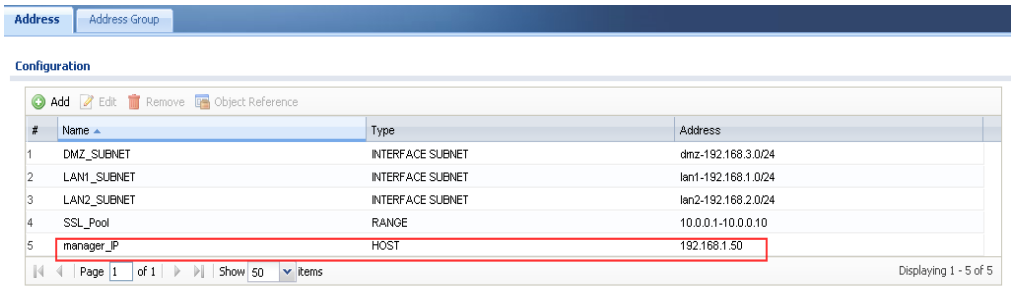
10.3 Configuration Guide

Network Conditions:

- LAN subnet: 192.168.1.0/24
- Manager IP: 192.168.1.50

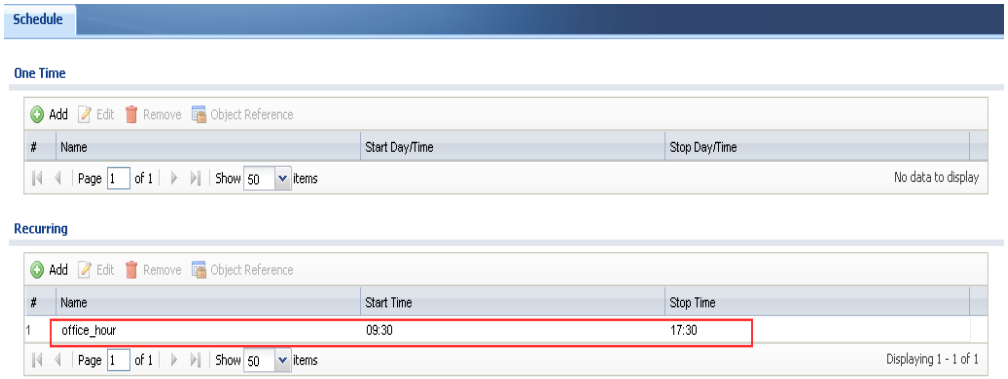
Goals to achieve:

1) The manager can access all websites at any time.
2) During office hours, other employees should be restricted from accessing websites that are irrelevant to their work.
3) All employees may access any websites outside of office hours.

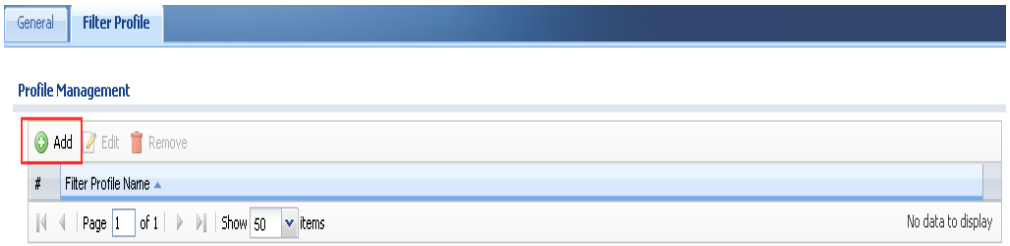
ZLD configuration	ZyNOS configuration
Step 1. Go to **Configuration> Object > User/Group**. Add an address object for the manager's IP.  	Step 1. Go to **SECURITY > CONTENT FILTER > General**. First of all, please make sure Content Filter service is licensed. Enable Content Filter. Enable **External Database Content Filtering** and set the action for matched web pages to "**Block and Log**". Enter **the message to display when a website is blocked**. E.g. "This website is restricted. Please contact administrator."

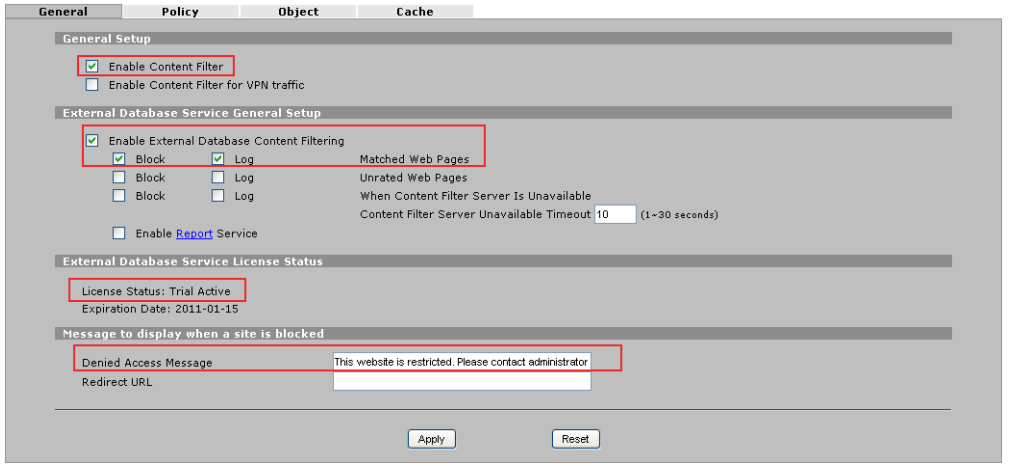
All contents copyright (c) 2010 ZyXEL Communications Corporation.

Step 2. Go to **Configuration > Object > Schedule**. Add a Recurring schedule for office hours.

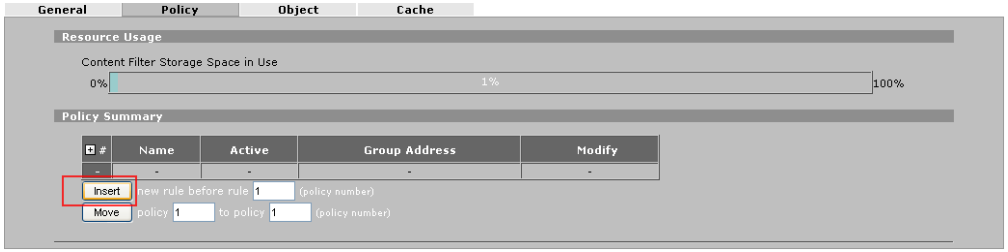

Schedule
One Time
Add Edit Remove Object Reference
Name Start Day/Time Stop Day/Time
Page 1 of 1 Show 50 items
No data to display
Recurring
Add Edit Remove Object Reference
Name Start Time Stop Time
1 office_hour 09:30 17:30
Page 1 of 1 Show 50 items
Displaying 1 - 1 of 1

Step 3. Go to **Configuration > Anti-X > Content Filter > Filter Profile**. Add a profile.




General Policy Object Cache
General Setup
Enable Content Filter
Enable Content Filter for VPN traffic
External Database Service General Setup
Enable External Database Content Filtering
Block Log Matched Web Pages
Block Log Unrated Web Pages
Block Log When Content Filter Server Is Unavailable
Content Filter Server Unavailable Timeout 10 (1~30 seconds)
Enable Report Service
External Database Service License Status
License Status: Trial Active
Expiration Date: 2011-01-15
Message to display when a site is blocked
Denied Access Message This website is restricted. Please contact administrator
Redirect URL
Apply Reset

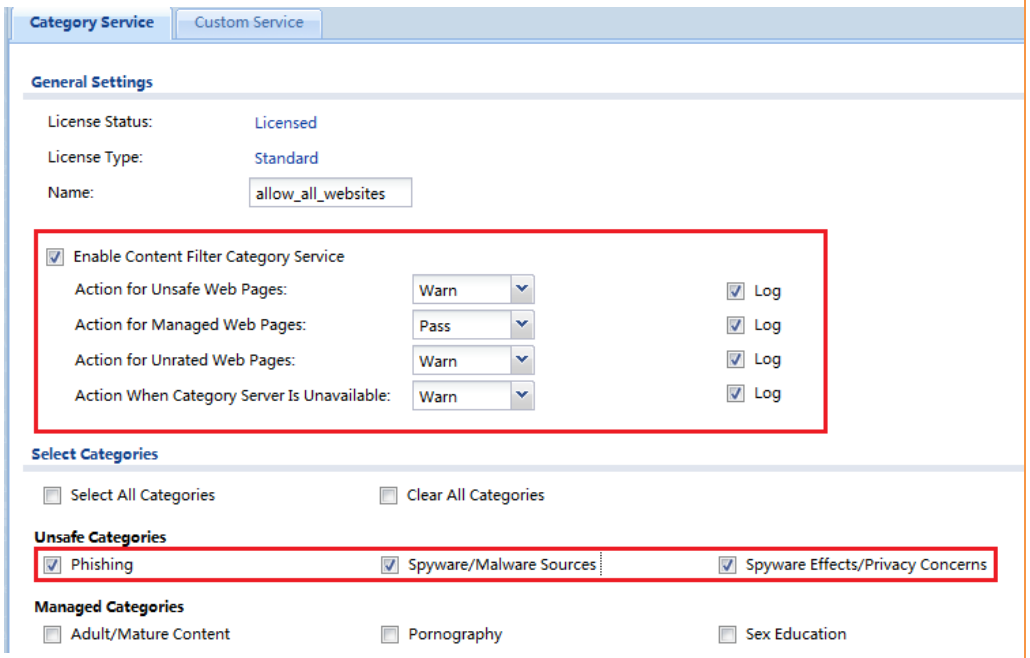
Step 2. Go to **SECURITY > CONTENT FILTER > Policy**.
Insert an access policy.


General Policy Object Cache
Resource Usage
Content Filter Storage Space in Use
0% 1% 100%
Policy Summary
Name Active Group Address Modify
Insert new rule before rule 1 (policy number)
Move policy 1 to policy 1 (policy number)

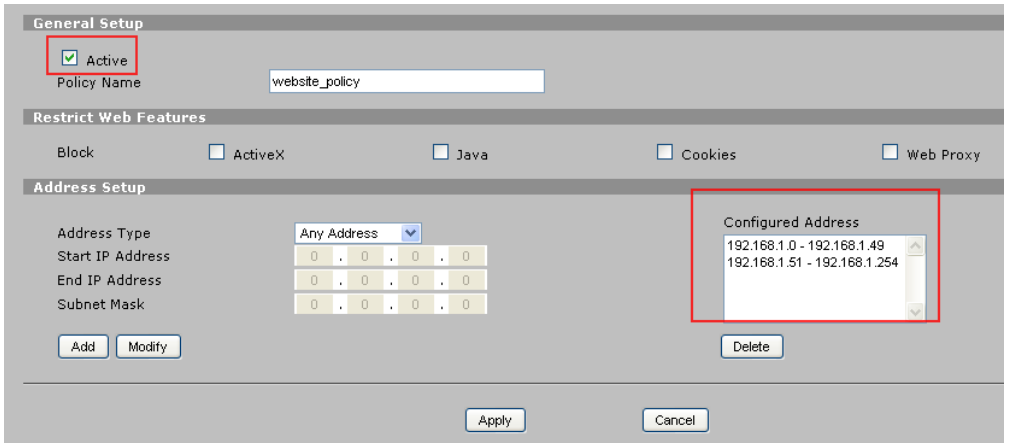
All contents copyright (c) 2010 ZyXEL Communications Corporation.

Add a profile which allows users to serf all websites.

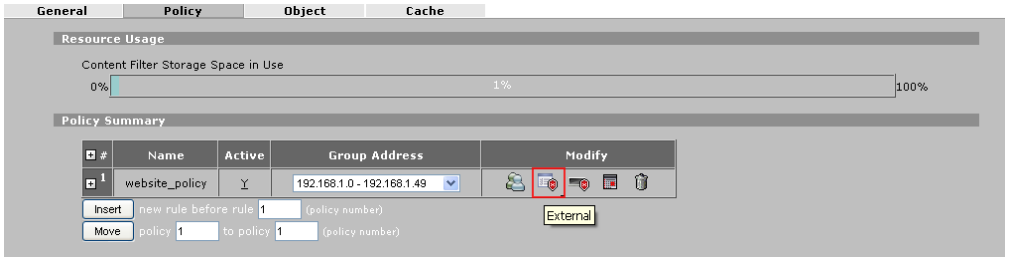
Enable **Content Filter Category Service**.
Set action for Unsafe Web Pages to “Warn and Log”.
Set action for Managed Web Pages to “Pass”.
Set action for Unrated Web Pages to “Warn and Log”.
Set action When Category Server is Unavailable to “Warn and Log”.
Check all the unsafe categories, and leave all the managed categories as unchecked.



Add a policy to meet the requirement that during office hours, employees should be prevented from accessing some websites, and that the manager (192.168.1.50) is not restricted.
Address Setup: Add two address ranges to Configured Address.
192.168.1.0~192.168.1.49
192.168.1.51~192.168.1.254



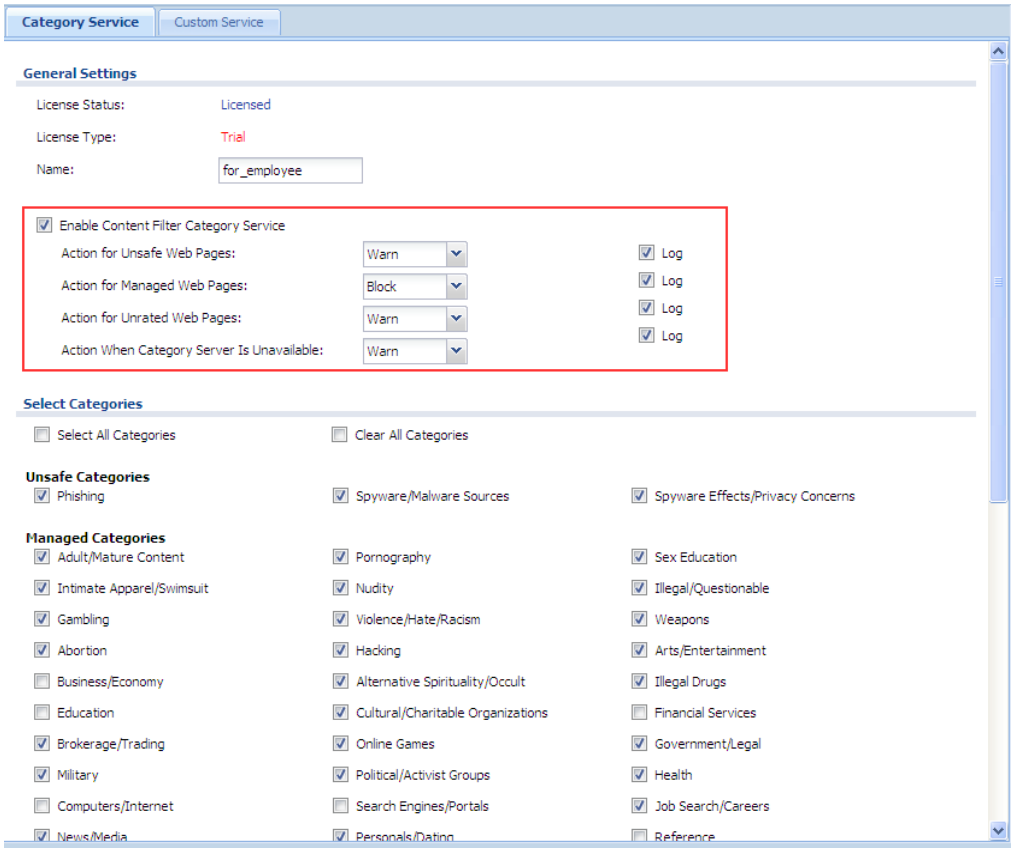
Click the External icon to edit the external categories.


General Policy Object Cache
Resource Usage
Content Filter Storage Space in Use
0% 1% 100%
Policy Summary
Name Active Group Address Modify
1 website_policy Y 192.168.1.0 - 192.168.1.49
Insert new rule before rule 1 (policy number)
Move policy 1 to policy 1 (policy number)
External

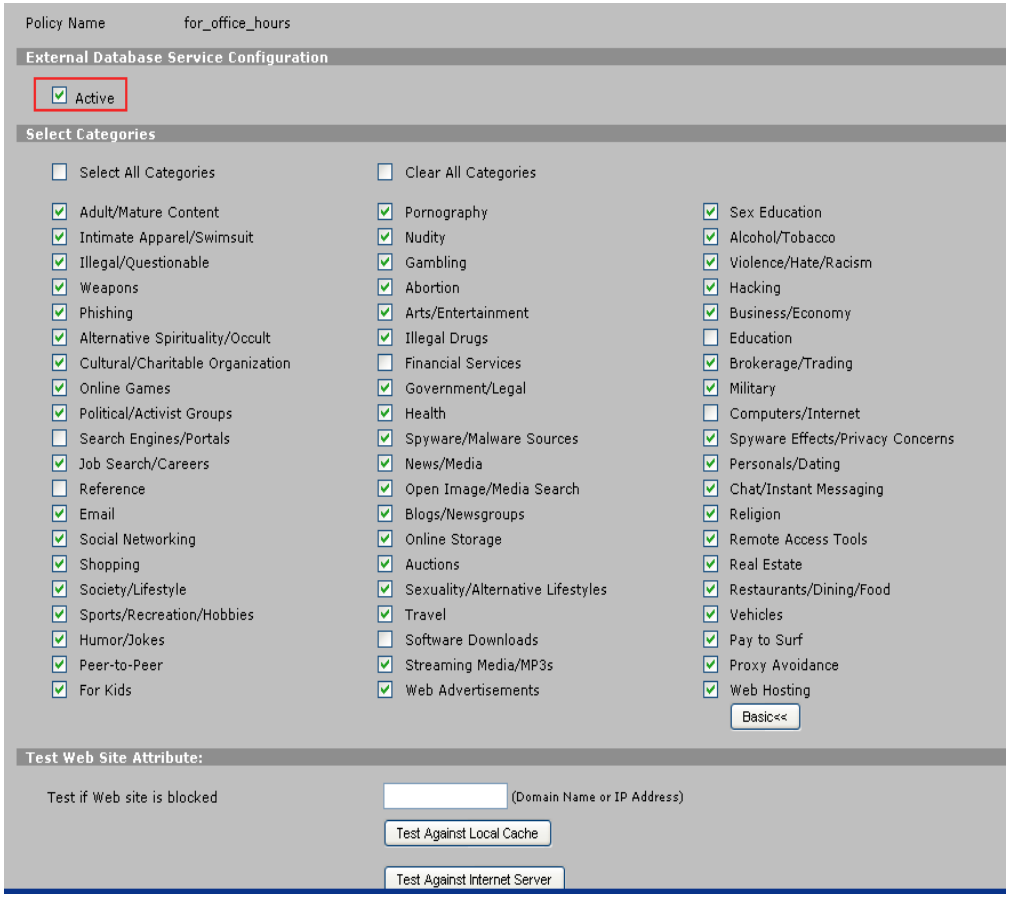
All contents copyright (c) 2010 ZyXEL Communications Corporation.

Add a profile for employees to surf only allowed websites.

Enable Content Filter Category Service.
Set action for Unsafe Web Pages to “Warn and Log”.
Set action for Managed Web Pages to “Block and Log”.
Set action for Unrated Web Pages to “Warn and Log”.
Set action When Category Server is Unavailable to “Warn and Log”.
Check all the unsafe categories.
Check the managed categories that you don’t want employees to surf during office hours.



Activate the **External Database Service**. Select managed websites that you want to prevent the employees from accessing during office hours.

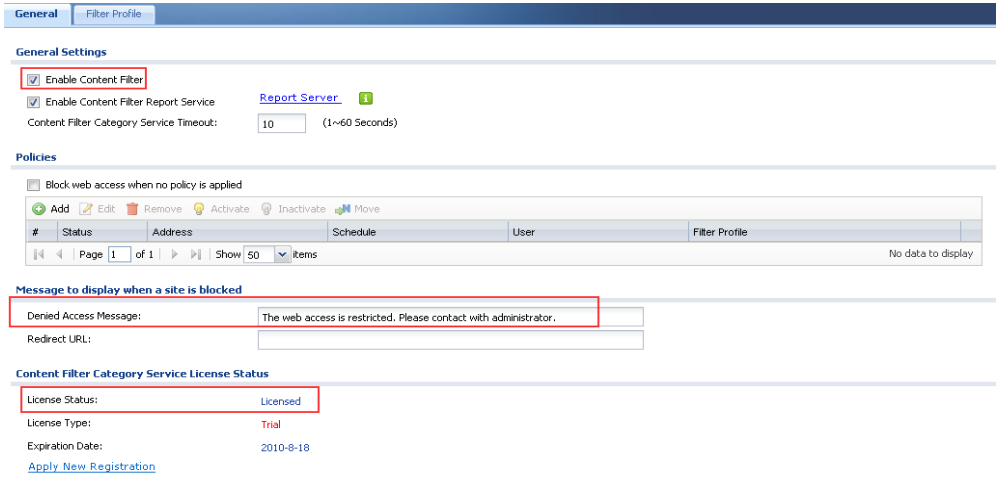


All contents copyright (c) 2010 ZyXEL Communications Corporation.

Step 4. Switch to **Configuration > Anti-X > Content Filter > General**. Enable **Content Filter**.

You can edit the **Denied Access Message**.

Make sure the Content Filter service is licensed.



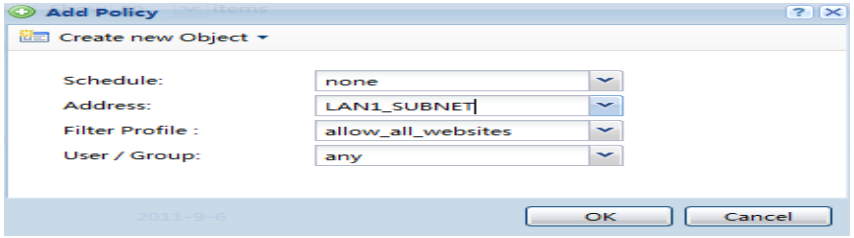
Add an access policy for all the crew outside of office hours.

Schedule: none.

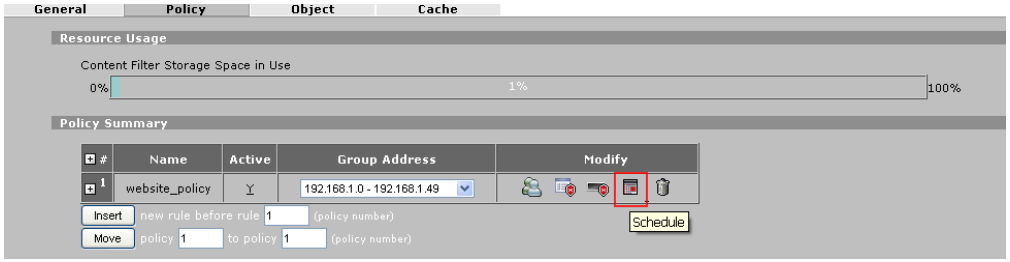
Address: select the address object LAN subnet.

Filter Profile: select the profile "**allow_all_websites**" created in the Profile page.

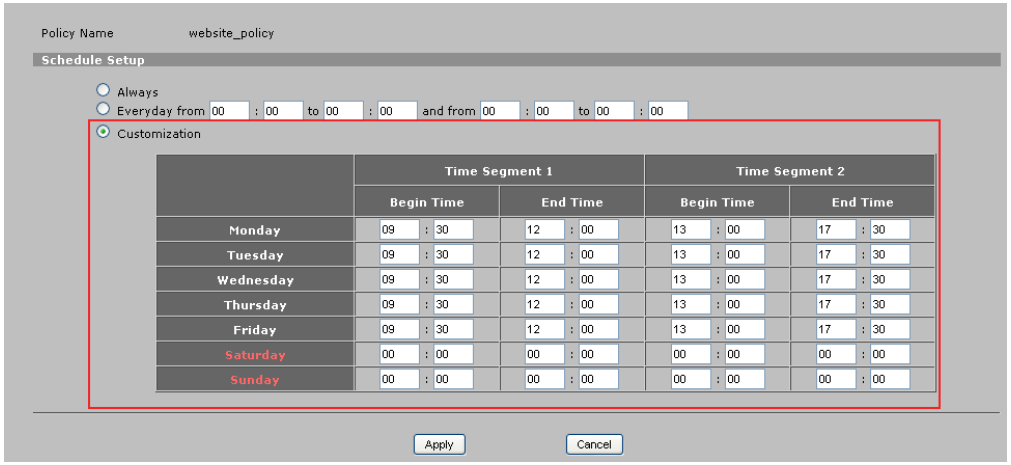
User/Group: Any



Click on the **Schedule** icon to edit the schedule.



Choose **Customization**, and define your office hours.



All contents copyright (c) 2010 ZyXEL Communications Corporation.

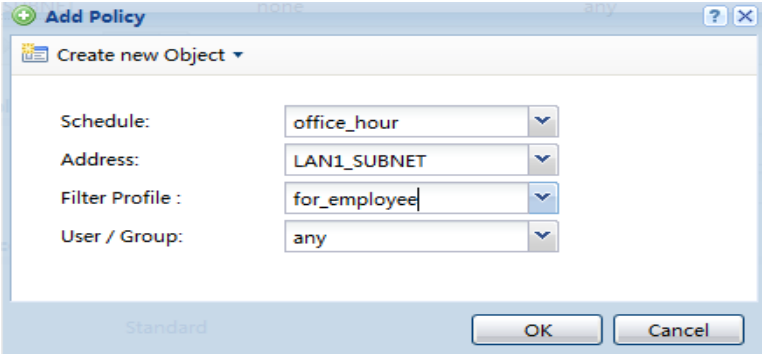
Add an access policy for the employees during office hours.

Schedule: select the “office_hour” object

Address: select the LAN subnet address object.

Filter Profile: select the “for_employee” profile created in the Profile page.

User/Group: Any

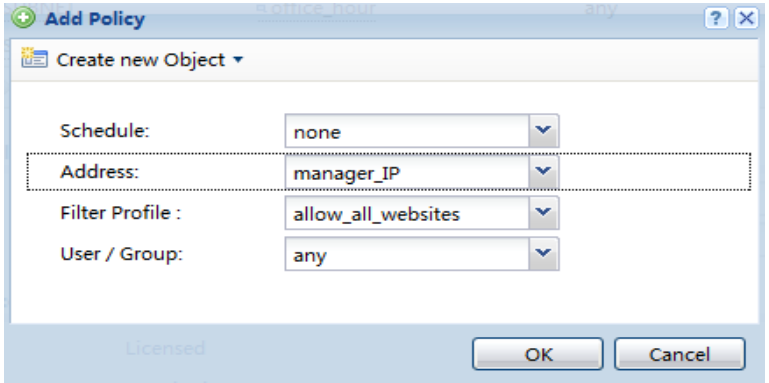


Add an access policy for the manager.

Schedule: none (all the time)

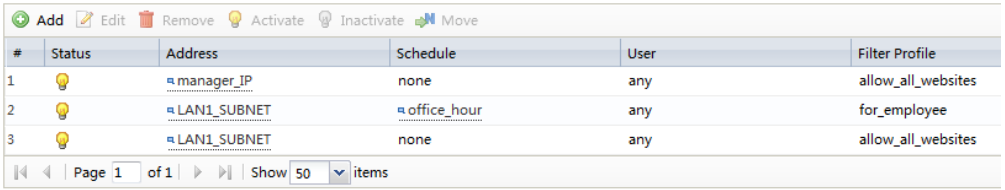
Address: manager’s IP address

Filter Profile: select the profile “**allow_all_websites**” created in Profile page.



All contents copyright (c) 2010 ZyXEL Communications Corporation.

Check the created policies. Make sure their order lists as below:

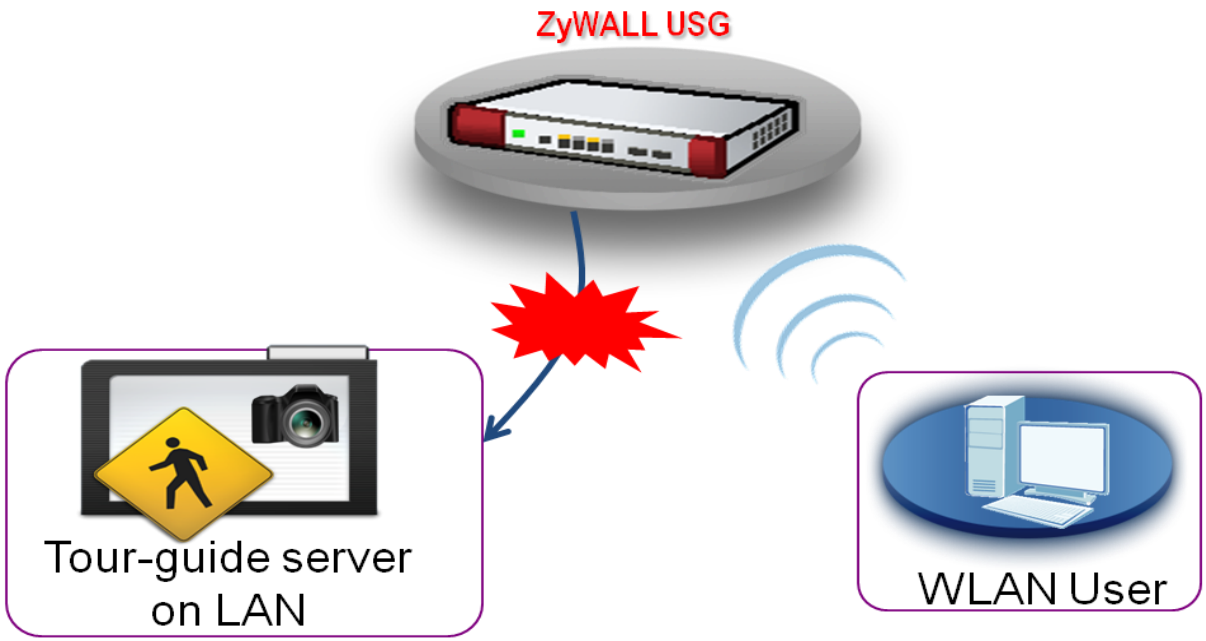


All contents copyright (c) 2010 ZyXEL Communications Corporation.

Scenario 11 — Quick Setup for Allowing WLAN Users to Access LAN Services

11.1 Application Scenario

To provide rich and helpful tour information to customers, most hotels have a tour guide server to present the message. However, due to the security protection design, WLAN users cannot access the server on LAN side by default. To enable this, the system administrator needs to configure the firewall policy to allow access from WLAN to LAN and also from LAN to WLAN. To streamline the configuration process, the administrator can simply relocate the WLAN users and the server on LAN side into the same security group to give them identical properties. The steps below will show you how to realize this.



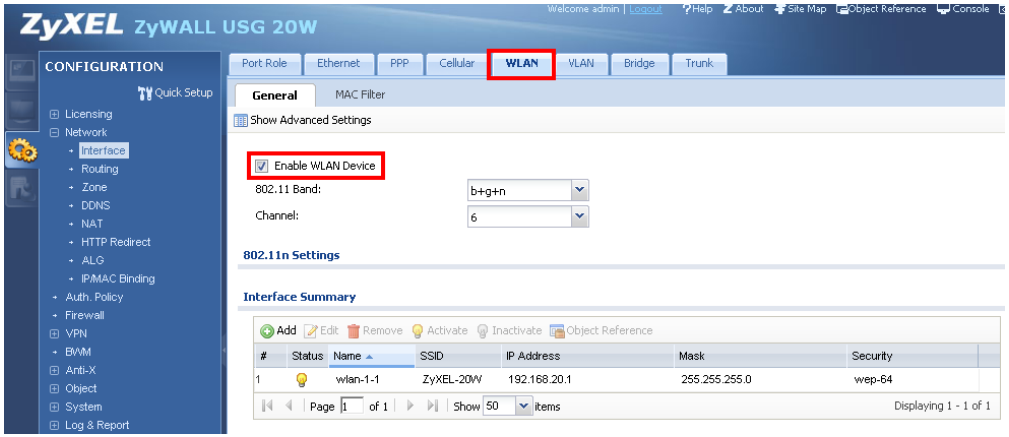
All contents copyright (c) 2010 ZyXEL Communications Corporation.

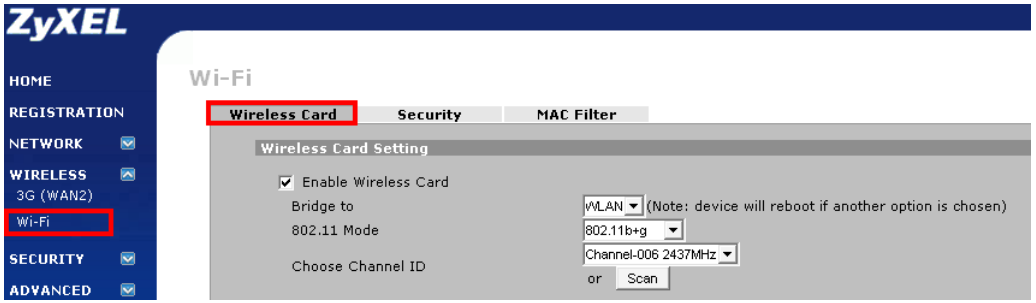
11.2 Configuration Guide

Goal to achieve:

A quick setup to allow users connected by WLAN access the service in the LAN zone.

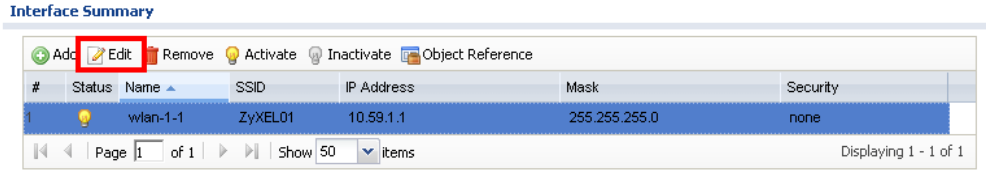
ZLD configuration	ZyNOS configuration
Step 1. Click **CONFIGURATION > Network > Interface > WLAN** to open the configuration screen.	Step 1. **Click WIRELESS > Wi-Fi > Wireless Card** to open the configuration screen.



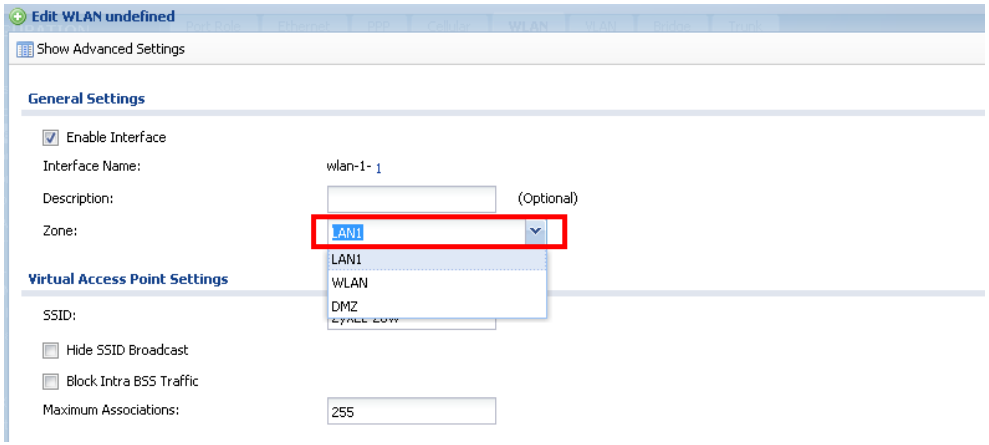


All contents copyright (c) 2010 ZyXEL Communications Corporation.

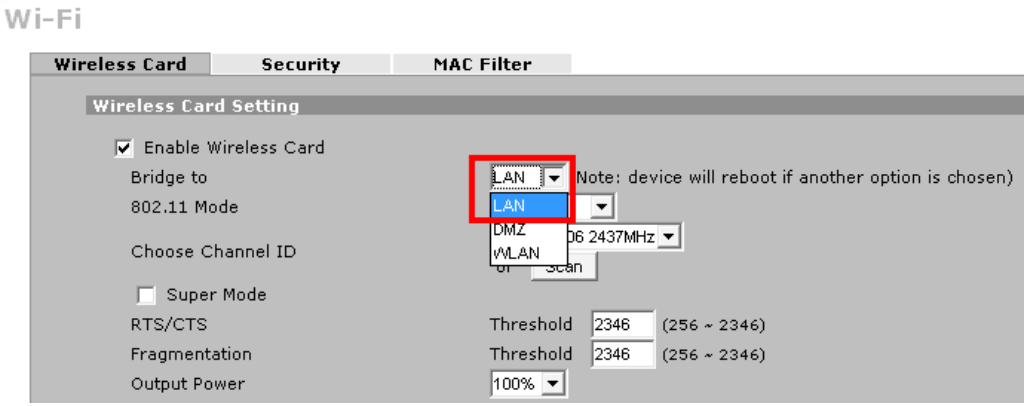
Step 2. You can add a new rule by clicking the **Add** button or edit the pre-configured rule by clicking the **Edit** button.



Step 3. Configure this SSID to belong to the LAN zone. With both the WLAN users and the LAN server belonging to the same security zone, the WLAN users will be able to access the LAN service even without modifying the firewall policy.



Step 2. Configure the WLAN bridge to the LAN zone. This will give the WLAN users the same security properties with the LAN server.



All contents copyright (c) 2010 ZyXEL Communications Corporation.